Приложение1
к приказу о проведении
государственных закупок способом ЗЦП

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ ЗАКУПАЕМЫХ УСЛУГ/САТЫП АЛЫНАТЫН ҚЫЗМЕТТЕРДІҢ ТЕХНИКАЛЫҚ ЕРЕКШЕЛІКТЕРІ

Наименование заказчика/Тапсырыс берушінің атауы : НАО «Кызылординский университет имени Коркыт Ата»/«Қорқыт Ата атындағы Қызылорда университеті» КЕАҚ
Наименование конкурса/Конкурс атауы: Государственные закупки способом запроса ценовых предложений на приобретение услуг по продлению лицензий на право использования антивирусного программного обеспечения / Антивирустық бағдарламалық қамтамасыз етуді пайдалану құқығына лицензияларды ұзарту жөніндегі қызметтерді сатып алуға баға ұсыныстарын сұрату тәсілімен мемлекеттік сатып алу
Общая выделенная сумма: 5 915 518 (Пять миллионов девятьсот пятнадцать тысяч пятьсот восемнадцать) тенге без НДС.
Жалпы бөлінген сома: 5 915 518 (Бес миллион тоғыз жүз он бес мың бес жүз он сегіз) теңге ҚҚС-сыз.

№	Атауы/ Наименование	Өлшембірлігі / Ед. изм.	Көлемі / Кол-во	Бірлігіүшінбағасы / Сумма за ед.	Жалпысомасы / Общая сумма
1.	**Наименование:** Услуги по продлению лицензий на право использования антивирусного программного обеспечения **Рабочие станции + ЦУ – 1300** **Сервер + ЦУ – 15** **Пользователей почты + ЦУ + Антиспам – 1000** **ОБЩИЕ ТРЕБОВАНИЯ** 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. Поставщик должен предоставить единый серийный номер для всех поставляемых продуктов. Поставляемый серийный номер должен иметь возможность отложенной активации. Срок действия лицензионных ключевых файлов на все поставляемые программные продукты должен начинаться с момента активации серийного номера. Наличие сертификата Государственной системы технического регулирования Республики Казахстан на поставляемый продукт, подтверждающего соответствие требованиям стандарта СТ РК ISO/IEC 15408-3-2017 по оценочному уровню доверия (ОУД4). **ТРЕБОВАНИЯ К ПРОГРАММНЫМ СРЕДСТВАМ** **ОБЩИЕ ТРЕБОВАНИЯ К АНТИВИРУСНОЙ ЗАЩИТЕ** Программные средства Системы должны обеспечивать определение угроз не менее следующих типов: классических вирусов, троянских программ, руткитов, сетевых червей, рекламных программ, программ автодозвона на платные сайты, потенциально опасных приложений, прочих вредоносных программ. Антивирусная защита должна обеспечивать: опознание вредоносных программ без запуска распаковщика - в целях ускорения проверки архивов и упакованных файлов; обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.; 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; обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME);	услуга	1	5 915 518	5 915 518

	обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, 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); 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, Da, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Or, Thunder Setup System, Wise Installation System, Alloy; 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; разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF; 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; 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; обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA); обнаружение угроз, направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля; обнаружение вредоносных объектов в DEX-файлах (Android); обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками. **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 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022, но и на рабочие станции под управлением MS Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11. Кроме того, должна быть реализована возможность установки сервера централизованного управления на ОС FreeBSD 10.3 и старше; а также Linux с версией библиотеки glibc 2.13 и выше. При этом сервер централизованного управления должен быть единым для всех защищаемых объектов, не зависимо от их операционных систем: Windows/Linux/macOS/Android. 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.				

	Аутентификация администраторов должна быть возможна следующими способами: из БД Сервера; с использованием LDAP/AD; с использованием RADIUS; с использованием PAM. 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 управления должна иметь возможность: объединения информации от нескольких серверов на одном; распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть; обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий; построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне. Должна быть реализована возможность запуска мобильного центра управления Системой на операционных системах iOS и Android с помощью соответствующих мобильных приложений, без использования веб-браузеров. 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, Postgres Pro, любая СУБД через ODBC-драйвер для операционных систем MS Windows и Linux; замены типа используемой СУБД в ходе работы, после установки серверной части – без необходимости переустановки серверной части Системы. управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов; в случае интеграции с внешними подсистемами с помощью встроенного Web API, должна иметься возможность аудита действий, произведенных с помощью функций данного Web API; самостоятельного написания обработчиков событий на языке Lua, а также выполнения произвольных Lua-скриптов с помощью средств системы управления; экспорта отчетов в форматы CSV, XML, HTML и PDF; подписки и получения новостей от компании разработчика, в том числе информирующих об актуальных угрозах, в консоли центра управления; наличия множественных путей уведомления пользователей и администраторов путем отправки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap; 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; ограничения сетевого трафика как при установке агентов, так и при их обновлении; скачивания конфигурационных файлов с настройками подключения антивирусных агентов для ОС Android, Mac OS X и ОС семейства UNIX; централизованного обновления антивирусных баз на всех защищенных рабочих станциях, в том числе мобильных и находящихся в режиме off-line. Доставки обновлений на рабочие места пользователей как по расписанию, так сразу после их получения; управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений; наличия возможности групповых обновлений; обновлений по защищенному каналу с использованием SSL-сертификатов;				

	организации отложенного обновления; автоматического перехода установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов; выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части; чтения полного пакета документации администратора и пользователя непосредственно в консоли центра управления. 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. 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. 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. 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. 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. 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. Выпуск обновлений вирусных баз производителем Системы не менее 20 раз в сутки, что должно подтверждаться созданным Системой отчетом; 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. Поддержка виртуальной инфраструктуры, интеграция с инфраструктурой виртуальных рабочих мест (VDI), поддержка гипервизоров VMware, Microsoft Hyper-V, Xen, KVM (Kernel-based Virtual Machine). **ТРЕБОВАНИЯ К ПРОГРАММНЫМ СРЕДСТВАМ АНТИВИРУСНОЙ ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ И СЕРВЕРОВ ПОД УПРАВЛЕНИЕМ ОС СЕМЕЙСТВА MICROSOFT WINDOWS** 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: MS Windows XP SP2 / Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.				

	MS Windows Server 2003 SP1 / Windows Server 2008 / Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022. Программные средства Системы должны обеспечивать осуществление антивирусной и антиспам защиты на рабочих станциях, включая постоянную защиту от руткит-технологий, наличие резидентного антируткит драйвера. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения. С целью противодействия вредоносным программам, запущенным на компьютере, для установки должен использоваться защищенный антируткитом инсталлятор (без использования Windows Installer). 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. 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. 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. 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. Система должна иметь возможность ограничения времени работы пользователей в сети Интернет, а также времени работы за компьютером. 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. 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. 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. 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. Фильтрация на уровне пакетов позволяющая контролировать доступ к сети Интернет вне зависимости от программ, инициирующих подключение. В Системе должна быть реализована превентивная защита, в дополнение к сигнатурному и эвристическому анализу, состоящая из таких компонентов как: защита от вымогателей – позволяющая защитить от троянцев-шифровальщиков;				

	защита от эксплойтов – позволяющая защитить от вредоносных объектов, пытающихся использовать уязвимости в популярных приложениях для проникновения в систему; 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. Возможность реализации защиты виртуальных рабочих мест с помощью установки виртуальных агентов. **ТРЕБОВАНИЯ К ПРОГРАММНЫМ СРЕДСТВАМ АНТИВИРУСНОЙ ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ И СЕРВЕРОВ ПОД УПРАВЛЕНИЕМ ОС СЕМЕЙСТВА LINUX** Поддержка процессоров следующих архитектур и систем команд: Intel/AMD: 32-бит (IA-32, x86); 64-бит (x86-64, x64, amd64); ARM64. Система, используя актуальную на момент проведения тендера версию ПО, должна обеспечивать защиту рабочих станций и серверов, использующих Samba версий 3.6.0, 4.0.0–4.10.0, под управлением операционных систем: Linux на основе ядра с версией 2.6.37 и новее, использующая PAM и библиотеку glibc версии 2.13 и новее. FreeBSD версии 9.x и выше. Интеграция Системы с Samba должна осуществляться с помощью модуля VFS (Virtual File System). 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. 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. Возможность установки и обновления Системы как через средства командной строки, так и с помощью графического инсталлятора. Возможность автоматической установки модулей, необходимых для установки необходимых компонентов Системы. Возможность установки компонентов Системы на зараженные вредоносными программами объекты без их предварительного лечения с последующим лечением заданных файловых областей. Поддержка подсистем обеспечения дополнительной безопасности SELinux, систем мандатного управления доступом PARSEC, а также режима замкнутой программной среды (ЗПС). Возможность мониторинга файловой системы с использованием как механизма fanotify, предоставляемого ОС, так и с помощью специального модуля ядра Linux (Linux kernel module). 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. Возможность управления использованием серверных ресурсов при выполнении сканирования файлового пространства. Возможность управления параметрами проверки составных файлов, таких, как архивы, почтовые файлы, упакованные объекты и прочие контейнеры. 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. В Системе должен быть реализован веб-фильтр с возможностью блокировки ресурсов Интернет по категориям, а также работы в режиме Белого/Черного списков.				

	Система должна поддерживать возможность порождения нескольких одновременно действующих процессов проверки. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей: поиск и удаление вирусов всех известных типов; антивирусного сканирования, заключающегося в полной или выборочной проверке на наличие угроз и проводимого как по команде администратора, так и по расписанию; антивирусной проверке «на лету» загружаемых файлов, как на сервер, так и с него; автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС; запуска задач по расписанию и/или сразу после загрузки операционной системы; настройки расписания сканирования с указанием параметров запуска. 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. 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). Возможность использования для проверки файлов метода потоковой проверки (flow), а также метода проксирования (proxy). Возможность проверки данных, не представленных в виде файлов, полученных через сеть, а также организации распределенной проверки файлов на наличие угроз. Возможность оперативной проверки на наличие угроз файлов, находящихся на локальном устройстве, с которого осуществляется доступ к веб-интерфейсу управления. 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. В состав Системы должен входить SNMP-агент, предназначенный для интеграции с системами мониторинга (Munin, Nagios, Zabbix). Интеграция в систему централизованного управления антивирусной защитой, позволяющая обеспечить управление системой антивирусной защиты «из одной точки» с максимальным удобством для системного администратора. **ТРЕБОВАНИЯ К ПРОГРАММНЫМ СРЕДСТВАМ АНТИВИРУСНОЙ ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ И СЕРВЕРОВ MACOS** 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. 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. Проверка объектов автозапуска, сменных носителей информации, сетевых и логических дисков, почтовых форматов, файлов и каталогов, включая упакованные и находящиеся в архивах. Мониторинг файловой системы в режиме реального времени, контроль запущенных программ и процессов, с возможностью исключения из проверки отдельных папок и файлов.				

	Мониторинг интернет-трафика в режиме реального времени по протоколам HTTP/HTTPS на содержание угроз, ограничение доступа к нерекомендуемым 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. Контроль всего входящего и исходящего сетевого трафика, блокировка доступа приложений к сетевым ресурсам согласно выбранному режиму работы и отдельным правилам фильтрации. Защита конфиденциальности с помощью контроля доступа приложений к веб-камерам и микрофонам. Использование системных уведомлений macOS, для отображения сообщений об обнаружении угроз, их обезвреживании или возникновении ошибок в работе компонентов. Возможность подключения к облачным сервисам компании-разработчика для защиты пользователей от инфицированных файлов и посещения нежелательных сайтов. **ТРЕБОВАНИЯ К ПРОГРАММНЫМ СРЕДСТВАМ АНТИВИРУСНОЙ И АНТИСПАМ ЗАЩИТЫ ПОЧТОВЫХ СИСТЕМ НА ПЛАТФОРМЕ MICROSOFT EXCHANGE** Система, используя актуальную на момент проведения закупки версию ПО должна функционировать на почтовых серверах: Microsoft Exchange Server 2007 x64 SP1 / 2010 x64 / 2013 SP1 Cumulative Update 5 / 2016 Cumulative Update 3 / 2019. Программные средства Системы должны обеспечивать защиту всей входящей и исходящей электронной корреспонденции, поступающей для обработки на почтовый сервер, как от вредоносных программ, так и от спама. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей: поддержка интерфейса Microsoft Virus Scanning Application Interface (VSAPI), проверка всех почтовых ящиков, включая служебные почтовые ящики SystemMailbox, System Attendant; возможность проверки в режимах: упреждающем (proactive); по запросу (on-demand); фоновом (background); поддержка серверных ролей: Сервер почтовых ящиков (Mailbox), Транспортный сервер-концентратор (Hub), Пограничный транспортный сервер (Edge); поддержка транспортных агентов: SMTP Receive Agent и Routing Agent; фильтрация и блокировка сообщений в зависимости от вероятности принадлежности их к спаму – по категориям: спам, вероятно, спам и маловероятно спам; обеспечение фильтрации почтового трафика на спам исключительно с использованием системы анализа на основе правил, не требующей постоянного обучения системы антиспама; изменение пороговых значений для определения принадлежности письма к той или иной группе спама; фильтрация по определенным типам сообщений и предотвращение массовых рассылок. Система должна поддерживать возможность создания правил фильтрации, в том числе фильтрацию по расширению, маске, размеру файла, максимальному количеству получателей писем; фильтрация файлов в архивах по их расширениям, и настройка применяемых к этим архивам действий; разбиение клиентов на группы для упрощения администрирования и задание с помощью профилей защиты, реализующих применение различных правил для групп, включая приоритет обработки; обеспечение возможности управления работой Системы с разными уровнями доступа; ведение журнала событий, в том числе с указанием необходимой степени детализации для определенного типа событий; отправка через протокол EWS (Exchange Web Services) почтовых уведомлений, содержащих информацию об отправителях, списке получателей и темах удаленных писем. **Сопутствующие услуги:** Сопутствующие услуги, такие как пуско-наладка и установка, включены в сумму закупки и осуществляются за счет поставщика.				

	Қызметтің атауы: Антивирустық бағдарламалық камтамасыз етуді пайдалану құқығына лицензияларды ұзарту жөніндегі қызметтер **Жұмыс станциялары + ЦУ – 1300** **Серверлер + ЦУ – 15** **Почта пайдаланушылар + ЦУ + Антиспам – 1000** **ЖАЛПЫ ТАЛАПТАР** Баскару құралдарын қоса алганда, барлық антивирустық құралдардың багдарламалық интерфейсі орыс және қазақ тілдерінде іске асырылуы тиіс. басқару құралдарын қоса алганда, Microsoft Windows отбасының операциялық жүйелерін басқарумен жұмыс істейтін барлық антивирустық құралдардың орыс және қазақ тілдерінде контекстік анықтамалық жүйесі болуы тиіс. Жеткізуші барлық жеткізілетін өнімдер үшін бірыңғай сериялық нөмірді ұсынуы тиіс. Жеткізілген сериялық нөмір кешіктірілген іске қосу мүмкіндігіне ие болуы керек. Барлық жеткізілетін багдарламалық өнімдерге арналған лицензияланған негізгі файлдардың жарамдылық мерзімі сериялық нөмір іске қосылған сәттен басталуы керек. 1.7 ҚР СТ ISO/IEC 15408-3-2017 сенімнің багалау деңгейі (ОУД4) бойынша стандартының талаптарына сәйкестігін растайтын жеткізілетін өнімге Қазақстан Республикасының Мемлекеттік Техникалық реттеу жүйесінің сертификатының болуы. **БАҒДАРЛАМАЛЫҚ ҚҰРАЛДАРҒА ҚОЙЫЛАТЫН ТАЛАПТАР** АНТИВИРУСТЫҚ ҚОРҒАУҒА ҚОЙЫЛАТЫН ЖАЛПЫ ТАЛАПТАР Жүйенің багдарламалық құралдары қауіптерді келесі түрлерден кем емес анықтауды қамтамасыз етуі керек: классикалық вирустар, трояндық багдарламалар, руткиттер, желілік құрттар, жарнамалық багдарламалар, ақылы сайттарға автоматты түрде қоңырау шалу багдарламалары, ықтимал қауіпті қосымшалар және басқа зиянды багдарламалар. Антивирустық қорганыс мыналарды қамтамасыз етуі керек: зиянды багдарламаларды декомпрессорды іске қоспай тану-мұрағаттар мен оралған файлдарды тексеруді жеделдету мақсатында; pklite, LZEXE, DIET, COM2EXE және т. б. сияқты багдарламалармен оралган файлдардан вирустарды анықтау және жою.; ACE форматындағы контейнерлер мен мұрагат файлдарының ішіндегі вирустарды анықтау (2.0 нұсқасына дейін), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (NRG, стандартты емес сектор форматындағы кескіндер және колтаңбасы жоқ), ZLIB, VCLZIP, VISE, PST, DMG, PDF, шифрланган контейнерлері бар GHOST INSTALLER және т. б. тексерілетін объектілердің кірістіру деңгейіне шектеусіз; қатаң форматы жоқ контейнерлердің ішіндегі вирустарды анықтау (HTML, MIME) ; нысан өлшемінің анық емес мәні бар контейнерлердің ішінде вирустарды анықтау (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES және т. б.); Smart Install Maker (Sim) форматы бар файлдар мен объектілерді антивирустық тексеру; DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 және одан жогары); SETUP FACTORY (7.8-жолдар); XENOCODE; TARMA INSTALL (3-жол); XZ (UNIX); COMPRESS; SQUAHFS; CHILKAT ZIP; LHA пакеттері (Award BIOS); өздігінен шығарылатын мұрагаттардағы антивирустық 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, Da, Setup Factory, setup Generator Pro, Sxa Zip, Tarma install, Or, Thunder Setup System, Wise Installation System. Alloy: pelock, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, rcryptor, pecrypt, сондай - ақ Mozilla				

	Thunderbird электрондық пошта файлдары-олардың өлшеміне қарамастан; пішімделмеген пошта базаларын талдау және жоғары кірістірілген хаттарды өңдеу (мысалы, көптеген жауаптар мен re/FW жіберулерімен хат алмасу), TNEF форматын қолдау; антивирустық базаларға тиісті ақпаратты енгізгеннен кейін құрылған және антивирустық зертханаларға талдауға әлі түспеген зиянды бағдарламалар отбасыларына тиесілі зиянды бағдарламалардан қорғау - эвристикалық талдау негізінде де, файлдағы код бөлімдерінің орналасуын талдауға негізделген ұқсас Вирустарды іздеу технологиясының көмегімен де; HTML және PDF құжаттарында зиянды объектілерді анықтау, соның ішінде осы типтегі құжаттарда орналасқан JavaScript - тегі эксплуатациялық эксплуатациялар. "Көрінбейтін" IFRAME элементтерін алу және талдау мүмкіндігі. Кез келген күрделіліктегі сценарийлерді тексеру және олардан қорғауды алып тастау мүмкіндігі; лицензиялық деректер бойынша қауіптерді анықтау (ASPROTECT, PEP және ENIGMA); 64 биттік операциялық жүйелерге, соның ішінде антируткит Модулінің Арнайы 64 биттік нұсқасымен бағытталған қауіптерді анықтау; DEX файлдарындағы зиянды нысандарды анықтау (Android); белгісіз орауыштардың астында жасырылған вирустарды анықтау және жою. **АНТИВИРУСТЫҚ ҚОРҒАУДЫ БАСҚАРУ ЖҮЙЕСІНЕ ҚОЙЫЛАТЫН ТАЛАПТАР** Жүйе тек MS Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022 серверлік ОЖ-де ғана емес, сонымен қатар MS Windows 7 / Windows жұмыс станцияларында да орталықтандырылған басқарудың антивирустық серверін орнату мүмкіндігімен клиент-сервер архитектурасы бойынша құрылуы керек 8 / Windows 8.1 / Windows 10 / Windows 11. Сонымен қатар, FreeBSD 10.3 және одан жоғары ОЖ-де орталықтандырылған басқару серверін орнату мүмкіндігі іске асырылуы керек; сонымен қатар Glibc кітапханасының 2.13 және одан жоғары нұсқасы бар Linux. Бұл ретте орталықтандырылған басқару сервері операциялық жүйелеріне қарамастан, барлық қорғалатын объектілер үшін бірыңғай болуы тиіс: Windows / Linux/macOS / Android. Басқару жүйесі Windows® Internet Explorer®, Microsoft Edge®, Mozilla® Firefox®, Google Chrome®, Opera®, Safari® (соның ішінде Microsoft Windows ОЖ, Linux, FreeBSD) браузерлерін қолдайтын кез келген операциялық жүйеден, браузерлердің соңғы нұсқаларын пайдалануға шектеусіз және толық орнатусыз қолжетімді болуы тиіс басқару серверінің жағында да, жүйенің әкімшісінің жағында да кез-келген бағдарламалық жасақтама. Әкімшілердің аутентификациясы келесі жолдармен мүмкін болуы керек: ДБ серверінен; LDAP / AD пайдалану; radius пайдалану; PAM пайдалану. Серверараралық байланыстар бойынша лицензияларды тарату мүмкіндігімен басқару серверлерінің - негізгі, бағыныстысы және тең құқылы иерархиялық жүйесін құру мүмкіндігі, сондай-ақ лицензиялық кілт файлын автоматты түрде жаңарту мүмкіндігі іске асырылуы тиіс. Басқару жүйесі болуы керек: бір серверде бірнеше серверлерден ақпаратты біріктіру; желіге жалпы жүктемені азайту мақсатында жаңартуларды алу үшін серверлер арасында жұмыс станцияларын бөлу; әр түрлі нұсқадағы антивирустық серверлер арасында бір иерархиялық желі шеңберінде Статистика алмасу; әкімшілер мен пайдаланушылардың рөлдерін, сондай-ақ әр деңгейде ұсынылатын есеп беру нысандарын теңшеу мүмкіндігі бар көп деңгейлі басқару жүйесін құру. Веб-шолғыштарды пайдаланбай, тиісті мобильді қосымшалардың көмегімен iOS және Android операциялық жүйелерінде жүйені				

	баскарудың мобильді орталығын іске қосу мүмкіндігі іске асырылуы тиіс. Басқару жүйесі болуы керек: сыртқы және ішкі ДҚБЖ-ны пайдалану (антивирустық сервер дистрибутивінің болігі ретінде жеткізіледі). Сыртқы ретінде Oracle, PostgreSQL, Postgres Pro, MS Windows және Linux операциялық жүйелеріне арналған ODBC драйвері арқылы кез-келген ДҚБЖ болуы мүмкін; жұмыс барысында пайдаланылатын ДҚБЖ түрін ауыстыру, сервер болігін орнатқаннан кейін-Жүйенің сервер болігін қайта орнатудың қажеті жоқ. дерекқорды басқару жүйесінің құралдарын басқару, оның ішінде Дерекқорды тазарту, оны талдау, ерікті SQL-сұрауларды орындау мүмкіндіктері; кірістірілген Web API комегімен сырткы ішкі жүйелермен интеграцияланған жагдайда, берілген Web API функциялары арқылы жасалған әрекеттерді тексеру мүмкіндігі болуы керек; оқиға өңдеушілерін Lua тілінде дербес жазу, сондай-ақ басқару жүйесінің комегімен ерікті Lua сценарийлерін орындау; есептерді CSV, XML, HTML және PDF форматтарына экспорттау; басқару орталығының консолінде әзірлеуші компаниядан, оның ішінде өзекті қауіптер туралы хабарлаушылардан жазылу және жаңалықтар алу; пошта хабарламасын, дыбыстық ескертуді, қалқымалы терезені, Оқиғалар журналына жазуды, SNMP-trap жіберу арқылы пайдаланушылар мен әкімшілерге бірнеше хабарлау жолдарының болуы; жүйелік әкімшінің еркін мазмұндағы пайдаланушыларға ақпараттық хабарламаларды жіберуі, оның ішінде: хабарлама мәтіні; интернет-ресурстарға гиперсілтемелер; жүйенің Web-интерфейсі арқылы нақты уақыт режимінде желі арқылы кез келген графикалық кескін; агенттерді орнату кезінде де, оларды жаңарту кезінде де желілік трафиктің шектеулері; Android, Mac OS X және UNIX отбасылық ОЖ үшін антивирустық агенттерді қосу параметрлері бар конфигурация файлдарын жүктеп алыңыз; барлық қорғалған жұмыс станцияларында, соның ішінде мобильді және Off-line режимінде орналаскан антивирустық базаларды орталықтандырылған жаңарту. Жаңартуларды кесте бойынша да, оларды алғаннан кейін де пайдаланушылардың жұмыс орындарына жеткізу; жаңартуларды кері қайтаруды қоса алғанда, антивирустық сервер репозиторийіндегі өнімдердің жаңартуларын тексеруді басқару; топтық жаңарту мүмкіндігінің болуы; SSL сертификаттарын қолдана отырып, қорғалған арна жаңартулары; кейінге қалдырылған жаңартуды ұйымдастыру; орнатылған бағдарламалық жасақтаманың жаңа нұсқаларға автоматты түрде ауысуы, оның ішінде жаңартылатын компоненттерді таңдау мүмкіндігі бар; антивирустық пакетті клиенттік бөліктерге орнатуды бастамас бұрын Орнатылатын компоненттерді таңдау және конфигурациялау; әкімші мен пайдаланушы құжаттамасының толық бумасын тікелей басқару орталығының консолінде оқыңыз. Жүйе мобильді пайдаланушылар үшін арнайы саясатқа ие болуы керек (Ноутбуктер), оны қолданған кезде мобильді пайдаланушылар антивирустық серверге қол жетімділік болмаған кезде антивирустық пакеттің параметрлерін редакциялауға және Интернет арқылы жаңартуға қабілетті болуы керек. Саясатты қолдану *типті конфигурация файлдарын қажет етпестен Web интерфейсі арқылы жүзеге асырылуы керек.xml. 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. Басқару жүйесінде жұмыс станцияларын анықтау және Active Directory, NetBIOS, ICMP, TCP бойынша іздеу режимдерінде				

	антивирустық агенттің болуын анықтау мақсатында желіні сканерлеуге мүмкіндік беретін компонент іске асырылуы тиіс. Басқару орталығында алдын ала орнатылған жүйелік және пайдаланушы топтары негізінде топтық саясат іске асырылуы тиіс. Алдын ала орнатылған жүйелік топтар: барлық қорғалатын объектілерге, Active Directory объектілері бойынша, операциялық жүйелер бойынша, саясаттар бойынша, параметрлер профильдері бойынша, желілік хаттамалар бойынша, объектінің мәртебесі бойынша, жеке параметрлер бойынша қол жеткізуге мүмкіндік беруі тиіс. Басқару жүйесінде тыйым салу және рұқсат беру ережелері негізінде де, қосымшаларды функционалды талдау негізінде де қосымшаларды іске қосуды бақылау мүмкіндігі болуы керек: қосымшаларды іске қосу, модульдерді жүктеу және орындау, сценарий аудармашыларын іске қосу, драйверлерді жүктеу, MSI пакеттерін орнату, орындалатын файлдардың тұтастығы. Жүйеде лицензия кілттерінің иерархиялық тізімін қолдайтын лицензия менеджері жүзеге асырылуы керек. Лицензия менеджері келесі мүмкіндіктерді ұсынуы керек: лицензия туралы ақпаратты қарау, жаңа лицензия кілтін қосу, лицензия кілтін жаңарту, лицензия кілтін ауыстыру, объектінің лицензия кілттерінің тізімін кеңейту, лицензия кілтін алып тастау және объектіні лицензиялау тізімінен алып тастау, лицензияларды коршілес басқару серверіне беру, коршілес басқару серверіне берілген лицензияларды өңдеу. Жүйе өндірушісінің вирустық базалардың жаңартуларын тәулігіне кемінде 20 рет шығаруы, бұл жүйе жасаған есеппен расталуы тиіс; Антивирустық серверлер Интернет желісіне кірмей ішкі желіде орналастырылған жағдайда, жаңартуларды алу репозиторийді офлайн жүктеудің арнайы утилитасын пайдалану арқылы мүмкін болуы тиіс. Виртуалды инфрақұрылымды қолдау, виртуалды жұмыс инфрақұрылымымен интеграция (VDI), VMware гипервизорларын қолдау, Microsoft Hyper-V, Xen, KVM (Kernel-based Virtual Machine). **MICROSOFT WINDOWS ОЖ БАСҚАРАТЫН ЖҰМЫС СТАНЦИЯЛАРЫ МЕН СЕРВЕРЛЕРДІ АНТИВИРУСТЫҚ ҚОРҒАУ БАҒДАРЛАМАЛЫҚ ҚҰРАЛДАРЫНА ҚОЙЫЛАТЫН ТАЛАПТАР** Жүйе (оның ішінде орталықтандырылған басқару жүйесінің көмегімен) тендер өткізу сәтінде озекті БҚ нұсқасын пайдалана отырып, операциялық жүйелердің басқаруындағы жұмыс станциялары мен серверлерді қорғауды қамтамасыз етуі тиіс: MS Windows XP SP2 / Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11. MS Windows Server 2003 SP1 / Windows Server 2008 / Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022. Жүйенің бағдарламалық құралдары руткит-технологиялардан тұрақты қорғауды, резидент антируткит драйверінің болуын қоса алғанда, жұмыс станцияларында антивирустық және антиспамдық қорғауды жүзеге асыруды қамтамасыз етуі тиіс. Жүйе оз компоненттерін вирустармен немесе басқа зиянды бағдарламалармен жұқтырылған желілік жұмыс станцияларына оларды алдын-ала емдеусіз орнату мүмкіндігін қолдауы керек. Компьютерде жұмыс істейтін зиянды бағдарламаларға қарсы тұру үшін орнату үшін антируткитпен қорғалған орнаткышты (Windows Installer қолданбай) пайдалану керек. Интернет желісіне кіру арнасының мүмкін болатын шектеулеріне байланысты қорғау жүйесін желіге кірусіз орнату мүмкін болуы керек Интернет-дистрибутивте қорғаныс жүйесінің барлық компоненттері, сондай-ақ қорғаныс жүйесімен реттелуі мүмкін Интернет желісінің зиянды бағдарламалары мен зиянды ресурстары белгілерінің дерекқоры болуы керек. Қорғаныс жүйесінің жұмысы үшін сыртқы кітапханалар, сондай-ақ.NET Framework ортасы пайдаланылмауы керек, олардың тұтастығы өзін-өзі қорғау жүйесінің бақылауында емес және защитыага келу қорғаныс жүйесінің ақпаратын көрсету қателеріне немесе қорғаныс жүйесінің интерфейсіне қатысты басқа мәселелерге әкелуі мүмкін.				

	Жүйенің құрамдас бөліктері файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін ДК ресурстарын пайдалануды басқара алуы керек, оның ішінде "оқуға" ашылатын файлдарды кейінге қалдырылған тексеру мүмкіндігі, сондай-ақ заманауи архитектуралардың ерекшеліктерін пайдалану. Жүйе жергілікті желіде және Интернетте Web-беттермен, электрондық поштамен, жергілікті қатты дискілермен және алынбалы медиамен, сондай-ақ желілік ресурстармен жұмыс істегенде антивирустық қорғауды қамтамасыз ететін конфигурацияда жеткізілуі тиіс. Кіріс және шығыс электрондық хат-хабарларды зиянды бағдарламалардан да, спамнан да қорғау қамтамасыз етілуге тиіс. Жүйе Интернет желісіндегі пайдаланушылардың жұмыс уақытын, сондай-ақ компьютерде жұмыс істеу уақытын шектей алуы керек. Пайдаланушылар үшін антивирустық пакет компоненттерінің параметрлеріне қол жеткізу құқықтарын жүйенің әкімшісі пайдаланушылардың дербес конфигурациялау мүмкіндігімен әкімші берген құқықтар шегінде және парольді қолданбай ғана айқындауы тиіс. Жұмыс станцияларын қорғау жүйесі жедел хабарламаларда трафикті сүзуді қамтамасыз етуі керек Mail.Ru agent, ICQ, Jabber, QIP, Pidgin және басқалары, соның ішінде жіберілген тіркемелерді антивирустық тексеру, сондай-ақ зиянды және фишингтік сайттарға апаратын сілтемелерді хабарламалардан автоматты түрде жою. Жұмыс станцияларын қорғау жүйесі Google, Yandex, Yahoo! іздеу жүйелерінің нәтижелерін беруді сүзуді қамтамасыз етуі керек., Bing, Rambler тек іздеу жүйелері мен ресурстарды қорғау жүйесі тұрғысынан қауіпсіз. Қолданба деңгейіндегі желілік қосылымдарды бақылау, нақты бағдарламалар мен процестердің желілік ресурстарға қол жетімділігін бақылауға және қолданбалар журналына кіру әрекеттері туралы ақпаратты тіркеуге мүмкіндік береді. Пакет деңгейіндегі сүзу қосылуды бастайтын бағдарламаларға карамастан Интернет желісіне кіруді бақылауға мүмкіндік береді. Жүйеде келесі компоненттерден тұратын қолтаңба мен эвристикалық талдаудан басқа, алдын-алу қорғанысы жүзеге асырылуы керек: ransomware қорғанысы-трояндық шифрлаушылардан қорғауға мүмкіндік береді; эксплуатациядан қорғау-жүйеге кіру үшін танымал қолданбалардағы осалдықтарды пайдалануға тырысатын зиянды нысандардан қорғауға мүмкіндік береді; мінез-құлықты талдау-хосттар файлы; жұмыс істеп тұрған қосымшалардың тұтастығы; дискіге төмен деңгейлі қол жетімділік; драйверлерді жүктеу; қосымшаларды іске қосу параметрлері; мультимедиялық құрылғы драйверлері; Winlogon қабықшасының параметрлері, Winlogon нотификаторлары; Windows қабығын автоматты түрде іске қосу; орындалатын файлдар қауымдастығы; іске қосуды шектеу саясаты бағдарламалар (SRP); Internet Explorer (BHO) плагиндері; бағдарламаларды автоматты түрде іске қосу; саясатты автоматты түрде іске қосу; Қауіпсіз режим конфигурациясы; Windows сеанс менеджерінің параметрлері; жүйелік қызметтер. Виртуалды агенттерді орнату арқылы виртуалды жұмыс орындарын қорғауды жүзеге асыру мүмкіндігі. **LINUX ОТБАСЫЛЫҚ ОЖ БАСҚАРАТЫН ЖҰМЫС СТАНЦИЯЛАРЫ МЕН СЕРВЕРЛЕРДІ АНТИВИРУСТЫҚ ҚОРҒАУ БАҒДАРЛАМАЛЫҚ ҚҰРАЛДАРЫНА ҚОЙЫЛАТЫН ТАЛАПТАР** Келесі архитектуралар мен командалық жүйелердің процессорларын қолдау: Intel / AMD: 32 бит (IA-32, x86); 64 бит (x86-64, x64, amd64); ARM64. 2Тендер өткізу кезінде БҚ-ның өзекті нұсқасын пайдалана отырып, жүйе операциялық жүйелердің басқаруымен Samba 3.6.0, 4.0.0–4.10.0 нұсқаларын пайдаланатын жұмыс станциялары мен серверлерді қорғауды қамтамасыз етуі тиіс:				

	2.6.37 және одан кейінгі нұсқасы бар ядрога негізделген Linux, PAM және glibc кітапханасының 2.13 және одан кейінгі нұсқаларын колданады. FreeBSD нұсқасы 9.х және одан жогары. Жүйені Samba-мен интеграциялау VFS (виртуалды файлдық жүйе) модулінің көмегімен жүзеге асырылуы керек. Жоғарыда айтылғандардан басқа Samba немесе Samba нұсқаларын қолданған жағдайда, Linux отбасының 64 биттік платформалары үшін интеграциялық модульдерді бастапқы кодтардан құрастыру мүмкіндігі болуы керек. Қолданылатын амалдық жүйенің түріне және нұсқасына, репозиторийге немесе ОЖ-де қолданылатын пакет менеджерімен жұмыс істеуге арналған пакетке тәуелсіз UNIX жүйелеріне арналған әмбебап пакеттен орнату мүмкіндігі. Пәрмен жолы құралдары арқылы да, графикалық Орнатушы арқылы да жүйені орнату және жаңарту мүмкіндігі. Жүйенің қажетті компоненттерін орнату үшін қажетті модульдерді автоматты түрде орнату мүмкіндігі. Жүйенің компоненттерін зиянды багдарламалармен залалданған объектілерге оларды алдын ала емдеусіз орнату, содан кейін берілген файлдық аймақтарды емдеу мүмкіндігі. Қосымша SELinux қауіпсіздігін қамтамасыз ететін ішкі жүйелерді, parsec мандатты қол жеткізуді басқару жүйелерін, сондай-ақ тұйық багдарламалық орта режимін (ЖЗҚ) қолдау. ОЖ ұсынатын fanotify механизмін де, арнайы Linux ядро модулін (Linux kernel module) қолдана отырып, файлдық жүйені бақылау мүмкіндігі. Файлдық жүйенің жаңа колемдерін (мысалы, USB-flash дискілерінде, CD/DVD дискілерінде, RAID массивтерінде және т.б.) орнату және жөндеу сәттерін автоматты түрде тану және қажет болған жағдайда бақыланатын аймақтар тізімін түзету мүмкіндігі. Файл кеңістігін сканерлеу кезінде серверлік ресурстарды пайдалануды басқару мүмкіндігі. Архивтер, пошта файлдары, оралған нысандар және басқа контейнерлер сияқты құрама файлдарды тексеру параметрлерін басқару мүмкіндігі. Жүйе SSL және TLS негізіндегі протоколдарды қолданатын қорғалған Желілік қосылыстар арқылы берілетін трафикті тексеру мүмкіндігімен орнатылған желілік қосылымдарды тұрақты басқару функциясын жүзеге асыруы керек. Жүйеде Интернет ресурстарын санаттар бойынша бұғаттау, сондай-ақ ақ/қара тізімдер режимінде жұмыс істеу мүмкіндігі бар веб-сүзгі іске асырылуы тиіс. Жүйе бір уақытта жұмыс істейтін бірнеше тексеру процестерін құру мүмкіндігін қолдауы керек. Жүйенің багдарламалық құралдары мынадай функционалдық мүмкіндіктерді іске асыруды қамтамасыз етуі тиіс: барлық белгілі типтегі Вирустарды іздеу және жою; қауіптердің бар-жоғын толық немесе іріктеп тексеруден тұратын және әкімші командасы бойынша да, кесте бойынша да жүргізілетін антивирустық сканерлеу; серверге де, одан да жүктелетін файлдарды "жылдам" антивирустық тексеру; антивирустық багдарламалық жасақтаманы және басқа да қажетті компоненттерді ОЖ жүктеуімен бірге автоматты түрде іске қосу; тапсырмаларды кесте бойынша және/немесе амалдық жүйе жүктелгеннен кейін бірден іске қосыңыз; іске қосу параметрлерін көрсететін сканерлеу кестесінің параметрлері. Багдарламаны басқару веб-интерфейс арқылы да, тікелей конфигурация файлдары арқылы да жүзеге асырылуы керек. Антивирустық тексеруге жататын файлдар мен каталогтарды, сондай-ақ әртүрлі типтегі зиянды объектілерге қатысты әрекеттерді көрсете отырып, антивирустық сканерлеу параметрлерін теңшеу мүмкіндігі. Сканерлеу ядросы дискілік құрылғылардың файлдары мен жүктеу жазбаларында вирустар мен басқа зиянды заттарды іздеуді қамтамасыз етуі керек (MBR - Master Boot Record, VBR - Volume Boot Record).				

	Файлдарды тексеру үшін ағынды тексеру әдісін (flow), сондай-ақ прокси әдісін (proxy) пайдалану мүмкіндігі. Желі арқылы алынған файлдар түрінде ұсынылмаған деректерді тексеру, сондай-ақ қауіп-қатерлерге файлдарды таратылған тексеруді ұйымдастыру мүмкіндігі. Басқару веб-интерфейсіне кіру жүзеге асырылатын жергілікті құрылғыда орналасқан файлдардың қауіптерін жедел тексеру мүмкіндігі. Қашықтағы желі түйіндерінде орналасқан файлдардың қауіптерін тексеру мүмкіндігі. Мұндай түйіндер тек жұмыс станциялары мен серверлер ғана емес, сонымен қатар Secure Shell немесе Telnet-ке қол жеткізуді қамтамасыз ететін "заттар интернетін" құрайтын маршрутизаторлар, теледидар консольдері және басқа да "ақылды" құрылғылар бола алады. Жүйенің құрамына бақылау жүйелерімен (Munin, Nagios, Zabbix) интеграциялауға арналған SNMP агенті кіруі керек. Жүйе әкімшісі үшін барынша ыңғайлылықпен "бір нүктеден" антивирустық қорғау жүйесін басқаруды қамтамасыз етуге мүмкіндік беретін антивирустық қорғауды орталықтандырылған басқару жүйесіне интеграциялау. **ЖҰМЫС СТАНЦИЯЛАРЫ МЕН MACOS СЕРВЕРЛЕРІН ВИРУСҚА ҚАРСЫ ҚОРҒАУ БАҒДАРЛАМАЛЫҚ ҚҰРАЛДАРЫНА ҚОЙЫЛАТЫН ТАЛАПТАР** MacOS-пен жұмыс істейтін құрылғыларды кез-келген қауіп-қатерден қорғау: вирустар, руткиттер, трояндық бағдарламалар, шпиондық бағдарламалар мен жарнамалық бағдарламалар, хакерлік утилиталар және әртүрлі зиянды заттар, қазіргі заманғы қауіп-қатерді анықтау және жою технологияларын қолдана отырып. Операциялық жүйелердің келесі нұсқаларында 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. Автоматты іске қосу объектілерін, ауыстырылатын ақпарат тасымалдағыштарды, желілік және логикалық дискілерді, пошта форматтарын, файлдар мен каталогтарды, соның ішінде оралған және мұрағаттағыларды тексеру. Нақты уақыт режимінде файлдық жүйені бақылау, жұмыс істеп тұрған бағдарламалар мен процестерді бақылау. Жеке қалталар мен файлдарды тексеруден шығару мүмкіндігі бар. HTTP/HTTPS хаттамалары бойынша нақты уақыт режимінде интернет-трафикті қауіп-қатердің мазмұнына, ұсынылмайтын сайттарға, сондай-ақ интернет-ресурстардың жекелеген сайттары мен санаттарына кіруді шектеуге, пайдаланушы айқындаған қосымшалар үшін жекелеген сайттар мен желілік қосылыстардың веб-трафигін тексеруден алып тастау мүмкіндігімен мониторингтеу. Барлық кіріс және шығыс желілік трафикті бақылау, таңдалған жұмыс режиміне және жеке сүзу ережелеріне сәйкес қолданбалардың желілік ресурстарға кіруін бұғаттау. Қолданбалардың веб-камералар мен микрофондарға кіруін бақылау арқылы құпиялылықты қорғау. Қауіптерді анықтау, оларды залалсыздандыру немесе компоненттердің жұмысында қателер туындағаны туралы хабарламаларды көрсету үшін macOS жүйелік хабарландыруларын пайдалану. Пайдаланушыларды жұқтырған файлдардан қорғау және қажетсіз сайттарға кіру үшін әзірлеуші компанияның бұлттық қызметтеріне қосылу мүмкіндігі. **MICROSOFT EXCHANGE ПЛАТФОРМАСЫНДА БАҒДАРЛАМАЛЫҚ ҚҰРАЛДАРҒА АНТИВИРУСТЫҚ ЖӘНЕ СПАМҒА ҚАРСЫ ПОШТА ЖҮЙЕЛЕРІН ҚОРҒАУҒА ҚОЙЫЛАТЫН ТАЛАПТАР**				

	Сатып алу кезінде багдарламалық жасақтаманың өзекті нұсқасын колданатын жүйе пошта серверлерінде жұмыс істеуі керек: Microsoft Exchange Server 2007 x64 SP1 / 2010 x64 / 2013 SP1 Cumulative Update 5 / 2016 Cumulative Update 3 / 2019. Жүйенің багдарламалық құралдары зиянды багдарламалардан да, спамнан да пошта серверіне өңдеу үшін келіп түсетін барлық кіріс және шығыс электрондық хат-хабарларды коргауды камтамасыз етуі тиіс. Жүйенің багдарламалық құралдары мынадай функционалдық мүмкіндіктерді іске асыруды қамтамасыз етуі тиіс: Microsoft virus Scanning Application Interface (VSAPI) қолдауы, барлық пошта жәшіктерін, соның ішінде systemmailbox, System Attendant қызметтік пошта жәшіктерін тексеру; режимдерде тексеру мүмкіндігі: алдын ала (proactive); сұраныс бойынша (d-demand); фондық (background); серверлік ролдерді қолдау: пошта жәшігі сервері (Mailbox), хаб-колік сервері (Hub), шекаралық колік сервері (Edge); колік агенттерін қолдау: SMTP Receive Agent және Routing Agent; хабарламаларды спамга тиесілі болу ықтималдығына карай сүзу және бұгаттау-санат бойынша: спам, мүмкін спам және екіталай спам; спамга пошта трафигін тек спамга қарсы жүйені үнемі оқытуды кажет етпейтін ережелерге негізделген талдау жүйесін қолдана отырып сүзуді қамтамасыз ету; хаттың белгілі бір спам тобына жататындығын анықтау үшін шекті мәндерді өзгерту; хабарламалардың белгілі бір түрлері бойынша сүзу және жаппай жіберілімдердің алдын алу. Жүйе кеңейту, Маска, файл өлшемі, электрондық поштаны алушылардың максималды саны бойынша сүзуді қоса алганда, сүзу ережелерін құру мүмкіндігін қолдауы керек; архивтердегі файлдарды олардың кеңейтімдері бойынша сүзу және осы архивтерге қолданылатын әрекеттерді конфигурациялау; басқаруды жеңілдету үшін клиенттерді топтарға бөлу және өңдеу басымдығын қоса алганда, топтар үшін әртүрлі ережелерді қолдануды жүзеге асыратын корганыс профильдері аркылы тапсырма беру; кол жетімділіктің әртүрлі деңгейлері бар жүйенің жұмысын басқару мүмкіндігін қамтамасыз ету; оқигалар журналын жүргізу, оның ішінде оқигалардың белгілі бір түрі үшін қажетті егжей-тегжейлі дәрежесін корсете отырып; жіберушілер, алушылар тізімі және Жойылган электрондық пошта тақырыптары туралы ақпаратты қамтитын EWS (Exchange Web Services) хаттамасы арқылы электрондық пошта хабарландыруларын жіберу. **Ілеспе қызметтер:** Іске қосу-баптау және орнату сияқты ілеспе қызметтер сатып алу сомасына енгізілген және жеткізушінің есебінен жүзеге асырылады.				
Всего:					**5 915 518**

Директор департамента экономики и финансов Н.Ж.Уразбаев

Руководитель управления инфраструктурных решений Б.М.Турсекеев

И.о. Руководителя управления правового обеспечения и государственных закупок Е.Б.Бесбай