**ИЗМЕНЕНИЕ В ДОКУМЕНТАЦИЮ О ЗАКУПКЕ**

**на проведение запроса котировок в электронной форме на право заключения договора**

**на поставку запасных индивидуальных принадлежностей для охранно-пожарной сигнализации, системы контроля управления доступом, систем оповещения, эвакуации и видеонаблюдения (ЗИП)**

**№ 61/18**

г. Москва «28» марта 2018 г.

Заказчиком Федеральным государственным унитарным предприятием «Московский эндокринный завод» принято решение о внесении изменений в Документацию и Извещение о закупке на проведение запроса котировок в электронной форме на право заключения договора на поставку запасных индивидуальных принадлежностей для охранно-пожарной сигнализации, системы контроля управления доступом, систем оповещения, эвакуации и видеонаблюдения (ЗИП)(номер закупки № 61/18), которые были опубликованы в Единой информационной системе в сфере закупок, номер извещения – № 31806282084 – 23.03.2018 г.

Внесены следующие изменения:

**В части изменения сроков:**

1. П. 6 Извещения о закупке (Дата и время окончания срока подачи заявок) «02» апреля 2018 г. 09:00 **изменить на** «04» апреля 2018 г. 09:00»;
2. п. 7 Извещения о закупке «Рассмотрение заявок на участие в закупке будет осуществляться «02» апреля 2018 года 12:00 по адресу: 109052, г. Москва, ул. Новохохловская, д. 23» **изменить на**: «Рассмотрение заявок на участие в закупке будет осуществляться «04» апреля 2018 года 12:00 по адресу: 109052, г. Москва, ул. Новохохловская, д. 23»;
3. п. 7 Извещения о закупке «Подведение итогов закупки будет осуществляться «02» апреля 2018 года по адресу: 109052, г. Москва, ул. Новохохловская, д. 23» **изменить на**: «Подведение итогов закупки будет осуществляться «04» апреля 2018 года по адресу: 109052, г. Москва, ул. Новохохловская, д. 23»;
4. п. 11 Извещения о закупке «Документация предоставляется с «23» марта по «02» апреля 2018 г.» **изменить на**: «Документация предоставляется с «23» марта по «04» апреля 2018 г.;
5. п. 12 части I «СВЕДЕНИЯ О ПРОВОДИМОЙ ПРОЦЕДУРЕ ЗАКУПКИ» «Дата окончания срока подачи заявок на участие в закупке является «02» апреля 2018 года в 09 часов 00 минут.» **изменить на**: «Дата окончания срока подачи заявок на участие в закупке является «04» апреля 2018 года в 09 часов 00 минут.»;
6. п. 14 части I «СВЕДЕНИЯ О ПРОВОДИМОЙ ПРОЦЕДУРЕ ЗАКУПКИ» «Участник закупки вправе направить заказчику запрос о разъяснении положений документации о закупке в соответствии с правилами и в порядке, установленным оператором электронной площадки с «23» марта по «29» марта 2018 года.» **изменить на**: «Участник закупки вправе направить заказчику запрос о разъяснении положений документации о закупке в соответствии с правилами и в порядке, установленным оператором электронной площадки с «23» марта по «02» апреля 2018 года.»;
7. п. 15 части I «СВЕДЕНИЯ О ПРОВОДИМОЙ ПРОЦЕДУРЕ ЗАКУПКИ» «Рассмотрение заявок на участие в закупке будет осуществляться «02» апреля 2018 года 12:00 по адресу: 109052, г. Москва, ул. Новохохловская, д. 23.» **изменить на**: «Рассмотрение заявок на участие в закупке будет осуществляться «04» апреля 2018 года 12:00 по адресу: 109052, г. Москва, ул. Новохохловская, д. 23.».
8. п. 15 части I «СВЕДЕНИЯ О ПРОВОДИМОЙ ПРОЦЕДУРЕ ЗАКУПКИ» «Подведение итогов закупки будет осуществляться «02» апреля 2018 года по адресу: 109052, г. Москва, ул. Новохохловская, д. 23.» **изменить на**: «Подведение итогов закупки будет осуществляться «04» апреля 2018 года по адресу: 109052, г. Москва, ул. Новохохловская, д. 23.».

**В части изменения содержания:**

1. **п.п. 4 «ПК (системный блок) Kraftway Credo KC44 Intel Core i7-7700, 2 x 8 ГБ DDR4-2133, Накопитель SSD 2.5" 250Gb Samsung 850 EVO SATA-III MZ-75E250BW, Видеокарта Gigabyte NVidia Ge Force GT730 GV-N730SL-2GL, Лицензия Kaspersky Antivirus for UEFI, KSS, ЭЗ "Витязь", Kaspersky UEFI, БП 450 Вт, Корпус MicroATX черный» п. 14 «Перечень и объем поставляемых ЗИП» части III «ТЕХНИЧЕСКОЕ ЗАДАНИЕ» изложить в следующей редакции:**

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | ПК (системный блок) Kraftway Credo KC44 Intel Core i7-7700, 2 x 8 ГБ DDR4-2133, Накопитель SSD 2.5" 250Gb Samsung 850 EVO SATA-III MZ-75E250BW, Видеокарта Gigabyte NVidia Ge Force GT730 GV-N730SL-2GL, Лицензия Kaspersky Antivirus for UEFI, KSS, ЭЗ "Витязь", Kaspersky UEFI, БП 450 Вт, Корпус MicroATX черный1 | 1 | шт |

1 Требования к аппаратно-программному комплексу:

Требования к аппаратно-программному комплексу:

Cистемный блок должен удовлетворять следующим требованиям:

• Скорость передачи данных по последовательной шине – не менее 8 GT/s;

• Системная плата

• не менее 2 (двух) DIMM слотов для оперативной памяти;

• поддержка 64-битных вычислений;

• поддержка до 32 ГБ оперативной памяти DDR4 -2133 МГц, с возможностью организации двухканального режима работы памяти;

• 1 (один) интегрированный сетевой контроллер 10/100/1000 Мб/с

• интегрированный SATA контроллер с поддержкой до:

• 4 (четырех) SATA портов 6.0 Гб/с на канал;

• с поддержкой режима AHCI, NCQ ;

• 1 (один) свободный слот PCI-Express 3.0 ×16;

• 1 (один) свободный слот PCI Express 2.0 ×1;

• внешние порты ввода/вывода:

• не менее 1 (одного) порта PS/2 для подключения клавиатуры и/или мыши;

• не менее 1 (одного) порта RJ-45;

• не менее 2 (двух) портов USB 3.0;

• не менее 4 (четырех) портов USB 2.0;

• не менее 1 (одного) порта VGA DSUB-15;

• не менее 1 (одного) порта DVI-D;

• не менее 1 (одного) порта HDMI;

• не менее 3 (трех) аудио разъемов mini-jack.

• внутренние порты ввода вывода(не менее):

• не менее 1 (одного) разъема 19-pin USB 3.0 ( 2 USB 3.0 порта);

• не менее 1 (одного) разъема 9-pin USB 2.0 ( 2 USB 2.0 порта);

• не менее 4 (четырех) разъёмов SATA;

• не менее 1 (одного) разъема 4-pin для подключения вентилятора охлаждения;

• не менее 1 (одного) разъема для датчика вскрытия корпуса

• базовая система ввода-вывода:

• тип базовой системы UEFI;

• возможность интеграции дополнительных модулей в UEFI BIOS;

• наличие встроенной в UEFI BIOS функции контроля целостности дополнительных модулей;

• возможность ведения в UEFI BIOS логов протокола работы дополнительных модулей с записью во встроенную энергонезависимую память, недоступную для чтения из операционной системы;

• наличие функции контроля целостности аппаратных компонентов с возможностью блокировки загрузки при обнаружении изменений в составе или свойствах аппаратных компонентов;

• наличие активированного интегрированного в UEFI BIOS модуля средства защиты от несанкционированного доступа;

• активированный интегрированный в UEFI BIOS модуль сканирования от вредоносного кода, работающий до загрузки операционной системы, с лицензией на 1 год

Требования к встроенному средству защиты от несанкционированного доступа:

• CЗИ от НСД, функционирующее до начала загрузки операционной системы, совместимое с UEFI BIOS версий 2.х и выше, должно выполнять следующие функции:

• предотвращение несанкционированного доступа к ресурсам компьютера;

• предотвращение загрузки операционной системы с внешнего носителя;

• контроль целостности программной среды компьютера с поддержкой файловых систем FAT16/32, NTFS, Ext2/3/4;

• встроенное средство формирования списков контроля целостности программной среды компьютера:

• должно поддерживаться формирование независимых списков проверки целостности программной среды;

• формирование списков должно проводится внутри оболочки замка без использования внешних утилит;

• должно поддерживаться управление списками для проверки (включение/выключение/удаление/модификация).

• регистрация событий доступа (в том числе несанкционированных) к ресурсам компьютера;

• СЗ от НСД должно отвечать следующим требованиям:

• обеспечивать режим двухфакторной аутентификации пользователей;

• обеспечить возможность добавления не менее 256 пользователей.

• вести журнал регистрации СЗ от НСД, который должен содержать исчерпывающую информацию о следующих событиях:

• успешная аутентификация;

• неуспешная аутентификация с сохранением ID предъявленного персонального средства аутентификации;

• нарушение целостности во время поверки списков контроля целостности программной среды компьютера;

• аудит действий администратора.

• служебная информация о пользователях (имя, описание), а так же журналы регистрации событий должны храниться в энергонезависимой памяти с возможностью сохранения на внешний носитель;

• защита кода СЗ от НСД должна осуществляться программно-аппаратными средствами материнской платы и должна обеспечивать следующие функции:

• защита от перезаписи кода UEFI, в том числе и методами восстановления образа UEFI из энергонезависимой памяти;

• защита от перезаписи настроек UEFI;

• защита журнала регистрации событий от несанкционированного чтения и записи из операционной системы;

• встроенный в UEFI сторожевой таймер;

• активация/деактивация СЗ от НСД должна осуществляться программно, без механических операций вскрытия и установки/извлечения компонентов.

• аутентификация пользователей СЗ от НСД должна проводиться с помощью идентификаторов следующих типов: электронных ключей, считывателей CCID со смарт-картами.

• СЗ от НСД должно сохранять работоспособность при замене ОС, для любых типов ОC.

• СЗ от НСД должно обеспечивать аутентификацию и идентификацию пользователей для каждой копии ОС независимо от типа и количества установленных в АРМ ОС.

• СЗ от НСД должно обеспечивать аутентификацию и идентификацию пользователей до запуска гипервизора в АРМ с виртуализированными ОС.

• СЗИ от НСД должен соответствовать требованиям:

• руководящего документа «Защита от несанкционированного доступа к информации.

Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4 уровню контроля;

• может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно, в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», Гостехкомиссия России, 1992г.;

Требования к интегрированному в UEFI BIOS модулю антивирусной защиты, работающего до загрузки операционной системы в АРМ.

1. Системные требования к антивирусной защите.

• Исполняемый код модуля сканирования не должен находиться на внешних по отношению к материнской плате дисковых хранилищах;

• Сканирование должно выполняться до выбора загрузочного носителя операционной системы;

• Антивирусное сканирование должно выполняться до запуска кода операционной системы;

• Антивирусная защита должна позволять выполнять сканирование критически важных областей операционной системы

• По должно поддерживають следующие файловые системы: FAT16/32, NTFS, EXT, EXT2, EXT3, EXT4.

• ПО должно поддерживать следующие операционные системы:

• ОС на дистрибутивах Linux:

1. Ubuntu Desktop 12.04.1 LTS x86

2. ALT Linux 7.0 Centaurus x64, x86

• ОС Windows:

1. Windows XP Professional (x86 и х64)

2. Windows 7 Embedded Standard 32-bit SP1

3. Windows 7 Professional (32-bit и 64-bit)

4. Windows 8 Professional (32-bit и 64-bit)

2. Функциональные требования к антивирусной защите.

• Определение угроз следующих типов:

• Классических вирусов;

• Буткитов;

• Руткитов;

• Сетевых червей;

• Троянских программ;

• Прочих вредоносных программ;

• Уведомление о найденных угрозах;

• Блокирование загрузки операционной системы или вывод сообщения на экран до загрузки операционной системы при обнаружении угрозы.

• Автоматическое обновление подсистемы проверки при наличии новой версии:

• новая версия подсистемы проверки доставляется на компьютер пользователя при очередном обновлении антивирусных баз;

• новая версия подсистемы проверки устанавливается только в случае успешной проверки целостности и подлинности;

• при возникновений ошибок в течение первого сеанса работы новой версии подсистемы проверки, производится автоматический возврат к последней стабильной версии подсистемы проверки.

• Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

• регламентное обновление антивирусных баз не реже 1 раза в течение календарных суток c использованием агента обновления работающего на уровне ОС;

• множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;

• проверку целостности и подлинности обновлений средствами электронной цифровой подписи до загрузки операционной системы.

3. Требования к методам антивирусного сканирования.

• Антивирусный модуль должен использовать следующие методы для обнаружения вредоносных объектов:

• Статические методы антивирусной защиты:

• сигнатурный анализ или использование сигнатур вредоносных объектов;

• проверка контрольной суммы файла;

• Проактивные методы антивирусной защиты:

• Крипто-анализ;

• Эвристический анализ;

• Эмуляция кода и эвристический анализ.

• Сигнатурный анализ объектов, направленный на обнаружение «семейств» вирусов

• Анализ объектов, направленный на обнаружение вредоносного кода, не являющегося вирусом (эксплойты, троянские программы, бэкдоры, буткиты/руткиты).

В комплекте с системным блоком должно быть предусмотрено программное обеспечение мониторинга и управления, внесенное в Единый Реестр Российских Программ для электронных вычислительных машин и баз данных, реализую¬щее следующие функции:

• Все операции управления и мониторинга должны выполняться дистанционно и централизованно из единой консоли;

• Веб-интерфейс для удаленного и централизованного мониторинга с поддержкой браузеров Internet Explorer, Mozilla Firefox, Google Chrome, Opera и шифрования (HTTPS);

• Реализация экспорта данных из внутренней базы данных в файлы формата XML, CSV и HTML;

• Журнал сервисных работ и событий;

• Возможность установки вручную пользовательского состояния системы после анализа ситуации;

• Импорт наблюдаемых объектов и их параметров из Excel и XML файлов, с возможностью последующей синхронизации с обновленным файлом;

• Описание адресов наблюдаемых систем с использованием базы данных адресов России (КЛАДР);

• Единая консоль сервера управления для мониторинга всех объектов инфраструктуры при работе распределенного сервера управления;

• Возможность распределения функции сервера мониторинга между несколькими физическими серверами, для уменьшения нагрузки на каждый из них при работе в больших инфраструктурах, а так же для расширения возможностей по масштабированию инфраструктуры управления;

• Мониторинг и оценку производительности сетевых сервисов; визуализация данных об изменении нагрузки;

• Мониторинг работоспособности почтовых серверов;

• Мониторинг сетевого SNMP совместимого оборудования;

• Автоматическое добавление наблюдаемых систем с использованием технологии Active Directory и сканированием по IP диапазону;

• Добавление в описание наблюдаемых систем произвольного количества дополнительных полей, с произвольными названиями и форматами;

• Отслеживание целостности интернет страниц с возможностью фильтрации по содержимому;

• Мониторинг сетевого Telnet совместимого оборудования

• Два режима инициации обмена данными со стороны сервера и со стороны агента;

• мониторинг инвентаризационной информации:

• версия BIOS;

• оптические приводы;

• порты COM и LPT;

• жёсткие диски, в том числе и находящиеся за RAID контроллерами;

• сетевые адаптеры;

• оперативная память;

• видеоадаптеры;

• аудиоадаптеры;

• процессоры;

• материнские платы;

• батарея;

• устройства Plug&Play (PCI,USB)

• инвентаризация:

• сбор и отображение информации об аппаратной конфигурации системы;

• сбор и отображение информации об установленном ПО;

• регулярное, автоматическое отслеживание изменений инвентаризационной информации;

• занесение данных об изменениях в системный журнал событий;

• создание инвентаризационных отчетов, отчетов по изменениям инвентаризационной информации, отчетов о производительности системы

• создание и отправка отчетов по заданному расписанию

• дистанционный мониторинг и отображение информации о текущей загрузке процессоров, оперативной памяти, дисков и сетевых интерфейсов, а также построение графиков по прошедшим событиям с детализацией по всем запущенным процессам;

• предсказательный анализ сбоя аппаратных компонентов систем, а именно:

• процессоров;

• жёстких дисков, в том числе и находящихся за RAID контроллерами; ;

• дистанционный анализ предсказания сбоев должен производиться автоматически на регулярной основе;

• дистанционный мониторинг и отображение информации о текущих запущенных процессах ПО, системных службах и драйверах ОС, а также загрузке системы, потребляемой виртуальной и реальной памяти, времени ядра;

• построение графиков по прошедшим событиям с детализацией по всем запущенным процессам;

• автоматическое дистанционное отслеживание запуска заданных приложений на наблюдаемой системе, с оповещением администратора и записью события в системный журнал;

• Мониторинг функционирования БД Oracle и MS SQL Server, журналов резервного копирования и оповещение о критических событиях;

• Получение снимка экрана с наблюдаемых ПК с возможностью сохранения в файл ;

• Мониторинг и управление терминальными станциями Kraftway;

• Контроль доступности наблюдаемых систем по сети с возможностью выполнения операции синхронно по группе наблюдаемых систем;

• Сбор данных о текущих локальных и удаленных пользователях системы: имя пользователя, имя рабочего ПК, прав пользователя, данных о сессии.

• Регистрация и оповещение о событиях входа локальных и удаленных пользователей; (Windows/Linux)

• Сбор журналов событий ОС и информирование об их переполнении; (Windows/Linux)

• Контроль использования программных продуктов

• Оповещение администратора различными способами:

• по электронной почте;

• отправка СМС;

• через внешние интернет-сервисы СМС-рассылок;

• через ловушки SNMP сообщений;

• Мониторинг функционирования серверной части продукта, оповещение о критических событиях;

• Служба поддержки пользователей через облачный сервис;

• Панель текущего состояния системы, позволяющая оперативно отслеживать срабатывания событий на наблюдаемых системах;

• Ранжирование событий по важности;

• Отслеживание и автоматическое информирование о следующих аппаратных событиях:

• критические изменения температуры;

• критические изменения напряжения;

• критические изменения скорости вращения вентиляторов;

• Отслеживание и автоматическое информирование о следующих системных событиях:

• перезагрузка системы;

• потеря связи с сетью;

• изменение состояния батареи;

• нехватка свободного пространства на дисках;

• нехватка виртуальной памяти;

• изменение системного времени;

• запуск и остановка системных служб и процессов;

• установка и удаление программного обеспечения;

• изменение инвентаризационной информации;

• локальный и удаленный вход пользователей;

• изменение целостности файлов и каталогов;

• Настройка порогов реакции для регистрации событий и настройка автоматической реакции для устранения возникшей проблемы;

• Дистанционное включение (Wake-on-LAN), выключение и перезагрузка ОС;

• Загрузка и/или запуск файлов;

• Включение/выключение межсетевого экрана; (Windows)

• Блокировка доступа к USB устройствам по классам

• Управление политикой доступа (чтение/запись) к оптическим дискам и USB устройствам;

• Остановка процессов, запуск/останов и управление режимом старта служб ОС;

• Запуск удалённого рабочего стола;

• Дистанционная установка и обновление агента на группе наблюдаемых систем;

• Удаление файлов на жестком диске без возможности восстановить содержимое

• Возможность интеграции с различным ПО мониторинга и управления с использованием стандартных механизмов информационного взаимодействия на основе протокола WS-Management (DSP0226 DMTF);

• Автоматическое обновление драйверов;

• Автоматическая установка обновлений ОС по расписанию;

• Возможность создавать контрольные точки для восстановления системы;

• Восстановление предыдущего состояния системы;

• Автоматическое создание резервной копии системы на внешние носители, а также возможность откатывать систему к заводским настройкам;

• Ролевое разграничение доступа:

• Только для просмотра;

• Полный доступ и управление объектами наблюдения без права изменения системы;

• Полный доступ ко всем компонентам системы;

• Аутентификация пользователей системы:

• по электронным ключам ruToken и eToken;

• проверка подлинности Windows;

• через Kraftway Security Center;

• Разграничение прав доступа к операциям в консоли управления;

• Защита агента от изменения и удаления;

• Возможность работы консоли управления в режиме киоска

Настоящее Изменение размещается в Единой информационной системе в сфере закупок.

Дополнительную информацию можно получить по адресу: 109052, г. Москва ул. Новохохловская, д. 25. Контактное лицо: Лукашенко Алексей Валерьевич - тел. +7(495) 234-61-92 доб. 628, zakupkimez@yandex.ru

Директор М.Ю. Фонарев