**Протокол № ЗК-ДБ-173/2**

**рассмотрения и оценки котировочных заявок**

**(ОАО «КСК»)**

|  |  |
| --- | --- |
| **г. Москва** | **03 июня 2014 г.** |

1. Заказчик: Открытое акционерное общество «Курорты Северного Кавказа»   
   (далее - ОАО «КСК», ИНН 2632100740).
2. На заседании Единой комиссии присутствовали:

Горчев Олег Сергеевич, Шашкин Никита Артемович, Ветчинников Владимир   
Николаевич, Дубенко Павел Николаевич, Иванов Николай Васильевич, Канукоев Аслан Султанович, Канунников Денис Викторович, Голосов Дмитрий Александрович.

Отсутствовали: Зверева Наталья Алексеевна, Кузнецов Андрей Александрович.

На заседание Единой комиссии в качестве эксперта приглашен: начальник отдела корпоративной защиты и информационной безопасности – Слаута Артур Александрович.

Кворум имеется, заседание Единой комиссии правомочно.

1. Извещение о проведении запроса котировок размещено на официальном сайте: [www.zakupki.gov.ru](http://www.zakupki.gov.ru), на сайте Общества (Заказчика): [www.ncrc.ru](http://www.ncrc.ru) в 19:00 (мск)   
   19 мая 2014 года № ЗК-ДБ-173.
2. Наименование предмета запроса котировок: Право на заключение договора   
   на создание автоматизированной системы защиты конфиденциальной информации   
   в ОАО «КСК» и оказание услуг по ее технической поддержке.
3. Сведения о существенных условиях договора:

|  |  |
| --- | --- |
| **Предмет договора** | Создание автоматизированной системы защиты конфиденциальной информации в ОАО «КСК»  и оказание услуг по ее технической поддержке. |
| **Начальная (максимальная) цена договора** | 2 550 821,24 (Два миллиона пятьсот пятьдесят тысяч восемьсот двадцать один) рубль 24 копейки, без учета НДС.  В цену договора включены все расходы поставщика услуг на уплату сборов, налогов (помимо НДС) и иных обязательных платежей. |
| **Наименование, перечень оказываемых услуг/выполняемых работ** | В соответствии с Техническим заданием (Приложение № 1 к настоящему Протоколу). |
| **Место выполнения работ/оказания услуг** | г. Москва, Пресненская набережная, дом 12.;  Ставропольский край, г. Пятигорск, пр. Кирова, д. 82а. |
| **Условия оплаты** | В соответствии с Проектом договора. |
| **Срок действия договора** | 425 (Четыреста двадцать пять) календарных дней со дня заключения договора. |
| **Финансирование** | Собственные средства ОАО «КСК». |

1. До окончания указанного в извещении о проведении запроса котировок срока подачи котировочных заявок 16:00 (мск) 27 мая 2014 года поступило 2 (Две) котировочные заявки на бумажном носителе.
2. Процедура вскрытия конвертов состоялась в 16:30 (мск) 27 мая 2014 года.
3. Процедура рассмотрения и оценки котировочных заявок состоялась в 17:00 (мск)   
   03 июня 2014 года по адресу: 123100, г. Москва, Пресненская набережная, д. 12.
4. Сведения об участниках закупки, подавших котировочные заявки:

| **Регистрационный номер заявки участника закупки** | **Наименование участника закупки** | **Юридический/почтовый адреса участника закупки** |
| --- | --- | --- |
| № 205  от 27 мая 2014 года 13:45 (мск) | **ЗАО «Андэк»**  (ИНН 7726585419) | Юридический адрес:  115162, г. Москва, ул. Хавская, д. 11  Почтовый адрес:  127083, г. Москва, ул. 8 Марта, д. 1, стр. 12, к. 5  Тел.: 8-495-280-15-50 |
| № 206  от 27 мая 2014 года 14:45 (мск) | **ЗАО «СофтЛайн Трейд»**  (ИНН 7736227885) | Юридический адрес/почтовый адрес:  119270, г. Москва, Лужнецкая наб., д. 2/4, стр. 3А, оф. 304  Тел.: 8-495-232-00-23 |

1. Результаты рассмотрения котировочных заявок на соответствие их требованиям, установленным в запросе котировок (Извещение от 19 мая 2014 года № ЗК-ДБ-173):
   1. Участник закупки **ЗАО «Андэк»** (ИНН 7726585419)не соответствует требованиям:

|  |  |  |
| --- | --- | --- |
| **№** | **Требование** | **Несоответствие** |
| 1. | В случае если котировочная заявка насчитывает более одного листа, все листы должны быть пронумерованы, **прошиты** и скреплены на прошивке печатью (для юридических лиц) и подписью уполномоченного представителя участника закупки. | Листы заявки не прошиты. |
| 2. | Вместе с котировочной заявкой, как приложения к котировочной заявке, участник закупки представляет:  - сведения об участнике запроса котировок с приложением копий документов, подтверждающие такие сведения. | В форме сведения об участнике запроса котировок отсутствует подпись главного бухгалтер. |
| 3. | 2.4. Участник закупки должен обладать необходимыми кадровыми ресурсами:  не менее 1 (одного) специалиста, имеющего необходимую для выполнения услуг по внедрению и технической поддержке ПО InfoWatch квалификацию: «Инженер внедрения  и поддержки InfoWatch Traffic Monitor 4.0.» (подтверждается гарантийным письмом);  не менее 1 (одного) специалиста по управлению проектами Project Management Professional или Project Management Expert (PMP/PME) (подтверждается гарантийным письмом). | Гарантийное письмо не представлено. |

Приглашенный эксперт (А.А. Слаута) подтверждает несоответствие требованиям, указанным в Извещении от 19 мая 2014 года № ЗК-ДБ-173.

* 1. Участник закупки **ЗАО «СофтЛайн Трейд»** (ИНН 7736227885) соответствует требованиям, указанным в Извещении от 19 мая 2014 года № ЗК-ДБ-173.

Приглашенный эксперт (А.А. Слаута) подтверждает соответствие требованиям, указанным в Извещении от 19 мая 2014 года № ЗК-ДБ-173.

1. **Решение:**
   1. В соответствии с п. 17.19 «Положения о закупке товаров, работ, услуг   
      для нужд ОАО «КСК», признать запрос котировок (Извещение от 19 мая 2014 года   
      № ЗК-ДБ-173) на право заключения договора на создание автоматизированной системы защиты конфиденциальной информации в ОАО «КСК» и оказание услуг   
      по ее технической поддержке несостоявшимся.

**Решение принято единогласно.**

* 1. На основании п. 17.20 «Положения о закупке товаров, работ, услуг для нужд   
     ОАО «КСК» рекомендовать Заказчику заключить договор с **ЗАО «СофтЛайн Трейд»** (ИНН 7736227885), с ценой договора **2 550 800** (Два миллиона пятьсот пятьдесят тысяч восемьсот) рублей, без учета НДС.

**Решение принято единогласно.**

* 1. Настоящий протокол подлежит хранению три года.

**Решение принято единогласно.**

1. Настоящий протокол подлежит публикации на официальном сайте: [www.zakupki.gov.ru](http://www.zakupki.gov.ru), официальном сайте Заказчика: [www.ncrc.ru](http://www.ncrc.ru) в сети Интернет.

Приложение:

1. Техническое задание – на 11 л., в 1 экз.

Председатель комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Горчев Олег Сергеевич

Заместитель

Председателя комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Шашкин Никита Артемович

Член комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ветчинников Владимир Николаевич

Член комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Дубенко Павел Николаевич

Член комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Иванов Николай Васильевич

Член комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Канукоев Аслан Султанович

Член комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Канунников Денис Викторович

Секретарь комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Голосов Дмитрий Александрович

Эксперт \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Слаута Артур Александрович

**Приложение № 1 к Протоколу  
от 03 июня 2014 года № ЗК**-**ДБ-173/2**

**Техническое задание**

1. Общие требования
   1. Основание для проведения закупки – Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации». Разработка ведется на основании данного технического задания и с учетом требований ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью», ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию», ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
   2. Сроки проведения работ:

* Начало – с даты подписания договора
* Окончание – длительность работ по внедрению Системы не должна превышать 60 (Шестьдесят) рабочих дней от даты подписания Договора с победителем конкурса.
  1. Исполнитель должен осуществить поставку программного обеспечения согласно Спецификации в Приложении №1 и создать систему защиты информации от внутренних угроз и утечек конфиденциальных данных (далее – Система) в ОАО «КСК» в объеме, предусмотренном настоящим Техническим заданием.

1. Назначение и цели создания системы
   1. Целью создания автоматизированной системы защиты конфиденциальной информации является обеспечение информационной безопасности в части обнаружения и реагирования на события Информационной Безопасности (далее - ИБ), возникающие в процессе обработки, хранения и перемещения конфиденциальной информации.

Создание Системы предназначено для совершенствования системы обеспечения ИБ Заказчика в части:

* мониторинг процесса передачи информации Заказчика через электронную почту, службы мгновенного обмена сообщениями, в сети Интернет за пределы организации;
* сканирование локальных дисков рабочих станций под управлением MS Windows, общедоступных сетевых ресурсов, файлового хранилища MS SharePoint;
* выявление фактов несанкционированной передачи, копирования на съёмные носители и печати информации сотрудниками Заказчика, контроль теневых копий файлов при данных операциях;
* расследование инцидентов, связанных с несанкционированной передачей конфиденциальной информации Заказчика, нелояльностью сотрудников Заказчика, нарушением законодательства с использованием вышеуказанных каналов передачи данных.

1. Исходные данные объекта автоматизации
   1. Количество рабочих станций – 200 шт.
   2. Характеристики инфраструктуры объекта автоматизации:

* Операционные системы, установленные на рабочих станциях пользователей – Microsoft Windows XP SP3, Microsoft Windows 7 и Windows 8;
* Система управления учетными записями – Microsoft Active Directory;
* Большое разнообразие используемых прикладных информационных систем (в т.ч. корпоративные почтовые системы, системы централизованного доступа в интернет, системы управления базами данных, корпоративные файловые хранилища и т.п.);
* Распределенная архитектура.

1. Требования к техническим и функциональным характеристикам создаваемой системы.
   1. Требования к структуре и функционированию Системы:
      1. Система должна иметь интерфейс централизованного управления и предоставления отчетности на русском языке;
      2. Функционировать в составе распределенной информационно-вычислительной сети;
      3. Функционировать по клиент-серверной схеме;
      4. Поддерживать кластерные технологии;
      5. Обеспечивать возможность подключения и обеспечения работоспособности на терминальных рабочих станциях.
      6. Обеспечивать возможность масштабирования.
      7. Обеспечивать возможность отказоустойчивости.
      8. Обеспечивать возможность модернизации путем замены технического и/или программного обеспечения;
      9. Обеспечивать возможность информирования администратора безопасности об инцидентах путем отправки письма-уведомления об инциденте на почтовый электронный адрес в режиме реального времени, а также выделением в системе инцидентов цветом, отличающимся от цвета корректных событий;
      10. Обеспечивать возможность интеграции со следующими proxy-серверами: Squid, Cisco IronPort, Bluecoat ProxySG, Microsoft Forefront TMG;
      11. Обеспечивать возможность интеграции со следующими смежными продуктами: DeviceLock, Microsoft Lync Server, Microsoft Exchange Server, ArcSight;
      12. Обеспечивать возможность интеграции и идентификации объектов с данными, полученными из Active Directory;
      13. Обеспечивать возможность использования Системы в структуре филиалов, соединенных любыми каналами связи, в том числе с низкой пропускной способностью;
      14. Для информационного обмена между компонентами системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP;
      15. Обеспечивать возможность контроля трафика удаленных элементов информационной системы.
      16. Обеспечивать управление загрузкой канала связи при взаимодействии с модулями Комплекса, расположенными в удаленных элементах информационной системы.
      17. Система должна функционировать в среде следующих операционных систем:
   * Microsoft Windows XP SP3 (32 bit)
   * Microsoft Windows 7 (32, 64 bit)
   * Microsoft Windows 8 (32, 64 bit)
   * Microsoft Windows Server 2003 (32 bit)
   * Microsoft Windows Server 2008 (64 bit)
   * Microsoft Windows Server 2008 R2 (64 bit)
   1. Требования к надежности:

* Обеспечивать возможность записи в журналы аудита информации по служебным событиям и сбоям. Записи в журналах должны содержать информацию, достаточную для установления причины неисправности;
* Обеспечивать штатное функционирование в случае одновременной работы всех пользователей на объекте автоматизации;
* Осуществлять резервное копирование и хранение резервных копий данных.
  1. Требования к защите информации от несанкционированного доступа:

Система должна иметь механизм разграничения доступа пользователей, с возможностью предоставления каждому пользователю Системы индивидуальных прав доступа.

* 1. Требования к персоналу:

Для использования системы защиты от внутренних угроз специалистам необходимо пройти сертифицированные курсы по обучению работе с системой у разработчика данной системы.

* 1. Требования к унификации:

Система должна иметь следующие сертификаты: ФСТЭК (НДВ4, ТУ, АС 1Г, ИСПДн К1), совместимости с eToken, Рутокен.

* 1. Требования к функционалу
     1. Система должна поддерживать каналы мониторинга данных:
* Электронная почта (SMTP-сообщения);
* Интернет (в том числе web-почта, форумы, мониторинг HTTP(s)-запросов);
* Системы мгновенных сообщений (ICQ, Skype, Mail.ru agent, Jabber);
* Мониторинг SIP (сообщения Microsoft Lync);
* Мониторинг распространения файлов по протоколу FTP;
* Разграничение прав доступа к периферийным устройствам (например: flash, usb-hdd, т.д.);
* Контроль копирования информации на периферийные устройства;
* Контроль печати (локальная, сетевая);
* Сканирование локальных дисков, сетевых папок, MS SharePoint на предмет наличия файлов нарушающих политики информационной безопасности;
* Система должна предоставлять возможность настройки скорости загрузки файлов, расписания и скорости сканирования;
* Предоставлять возможность блокировки данных, передаваемых по протоколам HTTP, HTTPS, SMTP;
* Мониторинг данных, передаваемых по протоколам HTTP, HTTPS, SMTP, OSCAR не должен требовать установки клиентского программного обеспечения;
* Возможность мониторинга голосовых сообщений Skype.
  + 1. Обеспечивать контроль сетевых соединений с возможностью запрета передачи данных по любым сетевым соединениям, кроме соединения с корпоративной сетью или с указанными разрешенными серверами.
    2. Для перечисленных в предыдущих пунктах поддерживаемых каналов мониторинга должна быть обеспечена возможность автоматической рубрикации извлеченного из объектов текста, с учетом морфологии, опечаток, транслитерации.
    3. Предоставлять возможность настраивать процесс рубрикации: задавать необходимые рубрики и их иерархию, а также признаки, по которым определяется релевантность анализируемого текста той или иной рубрике.
    4. Содержать предустановленные рубрики «Грифы конфиденциальности», «Структура компании», «Юридическая документация», «Финансовая служба» и др.
    5. Обеспечивать возможность автоматического создания описания рубрик на основе имеющихся примеров документов.
    6. Обеспечивать поддержание следующих видов фильтрации контента в режиме реального времени:
* классификация информации путем лингвистического анализа в соответствии с перечнем сведений составляющих конфиденциальную информацию;
* определение фактов передачи экземпляров конкретных текстовых и любых бинарных файлов/документов (предварительно определенных в Системе или цитат из них методом «Цифровых отпечаток»);
* детектирование фактов передачи текстовых объектов, сложных алфавитно-цифровых объектов (номера паспортов, индивидуальные номера налогоплательщиков, номеров кредитных карт, договоров или счетов в случае детектирования банковских реквизитов, кодов классификаторов и т.п.);
* автоматическое определение тематики текста на основании ключевых терминов и выражений;
* готовые шаблоны политик;
* детектирование фактов передачи изображений главной страницы внутреннего российского паспорта;
* детектирование фактов передачи эталонных выгрузок из баз данных;
* детектирование заполненных форм бланков, анкет, и т.п. типовых документов;
* детектирование эталонных печатей на изображениях отсканированных документов.
  + 1. Обеспечивать возможность распознавания текста в графических документах.
    2. Обеспечивать возможность автоматической рубрикации извлеченного из изображений текста, с учетом морфологии.
    3. Осуществлять фильтрацию «мусорного трафика» (бесполезных служебных http-запросов).
    4. Обеспечить возможность оперативного оповещения (по электронной почте) ответственных работников о зафиксированных событиях ИБ, а так же работников отправителей данных событий.
    5. Предоставлять возможности для автоматического вынесения вердикта по перехваченному объекту (выносимый вердикт должен трактовать, нарушает ли перехваченный объект политику безопасности или нет).
    6. Предоставлять возможности для задания правил автоматического вынесения вердикта по объекту. Должна обеспечиваться возможность применять правила автоматического вынесения вердикта на основании:
* формальных признаков (контекста) анализируемого объекта (отправитель, получатель и т.д.), в том числе типа анализируемого объекта (SMTP, HTTP(S), ICQ, Skype);
* результатов контентного анализа текста, извлеченного из анализируемого объекта (результаты рубрикации, сравнения с базой эталонных документов, поиска алфавитно-цифровых объектов и т.д.).
  + 1. Обеспечить устойчивость к следующим видам манипуляции с информацией:
* импортирование фрагмента конфиденциальной информации в документы, не являющиеся конфиденциальными;
* изменение порядка слов;
* изменения расстояний между словами;
* изменение форматирования документа;
* изменение словоформ;
* замены букв на символы другого алфавита;
* использование цифр вместо букв;
* изменение расширений файлов.
  + 1. Предоставлять возможности для автоматического проставления анализируемым объектам дополнительных атрибутов (на основании правил) (к дополнительным атрибутам относятся пользовательские теги, а также цвет, комментарии).
    2. Предоставлять возможности для детектирования и распаковки следующих типов объектов:
* детектирование: tiff, jpg, wmf/wmf31, emf, gif, mdb, mp3/mpeg3, wav, avi, wmv;
* предусмотреть возможность инспекции следующих видов архивов: gzip, bzip2, tar, arj, zip, rar, lha, zlib, 7z с глубиной вложенности до 100;
* детектирование и извлечение текста: MS Office (версия не ниже 2000; doc, docx, xls, xlsx, ppt, pptx, pps, ppsx, vsd), шаблонов MS Office (версия не ниже 2000; dot, dotx, dotm, xlt, xltx, xltm, pot, potx, potm), документов Adobe Acrobat (pdf), документов Open Office (odt, ods, odp), сообщений MS Outlook, документы rtf, html, Windows icon (ico), изображения emf;
* предусмотреть возможность настройки сигнатур, с помощью которых определяются типы файлов при распаковке вложений и архивов;
* поддерживать следующие кодировки: ISO-8859-1, ISO-8859-15, ISO-8859-5, win-1251, koi8-r, utf8.
  + 1. Обеспечивать хранение всей электронной корреспонденции (SMTP-сообщения электронной почты), сообщений и файлов, передаваемых через различные IM в том числе и сообщения MS Lync, POST-запросов, анализируемых файлов по протоколу FTP, анализируемых теневых копий файлов и заданий на печать в течение неограниченного срока.
    2. Позволять выгружать сегменты базы данных почтового хранилища на сменные носители или в хранилища данных с возможностью их последующего подключения и поиска по ним.
    3. Предоставлять возможности по разграничению доступа пользователей к анализируемым объектам (автоматическое отнесение анализируемого объекта к той или иной зоне ответственности на основании правил).
    4. Предоставлять возможности для управления зонами ответственности пользователей системы (в том числе для настройки маршрутов перемещения объектов между зонами ответственности).
    5. Предоставлять возможности управлять тегами и цветом, назначенными объекту (назначать/удалять).
    6. Предоставлять возможности задать комментарий для анализируемого объекта.
    7. Предоставлять возможности для подготовки статистических отчетов по анализируемым объектам в следующих форматах: xls, xlsx, pdf, csv, html, rtf, bmp, emf, wmf, gif, jpeg, png, tiff, txt.
    8. Обеспечивать контроль доступа пользователей к периферийным устройствам.
    9. Система должна предоставлять возможность настройки следующих правил для формирования политик безопасности:
* правил записи в файл на съемном устройстве;
* правил доступа к периферийным устройствам;
* правил печати;
* правил контроля сообщений, файлов и голоса, передаваемых с помощью Skype;
* правил контроля сообщений mail.ru agent, Jabber;
* правил передачи файлов по протоколу FTP;
* контроль сетевых подключений при работе за пределами корпоративной сети.
  + 1. Система должна предоставлять возможность создания белых списков устройств, доступ к которым разрешен.
    2. Система должна предоставлять возможность удаленной установки/обновления/удаления клиентских приложений системы контроля печати, записи файлов, перехвата сообщений, вложений, голосового трафика Skype, FTP, Mail.ru Agent, Jabber, доступа пользователей к периферийным устройствам.
  1. Требования к аппаратной платформе Системы

Аппаратная платформа должна обеспечивать:

* + Поддержку функционирования основных прикладных систем и задач Системы в соответствии с регламентом их эксплуатации и использования;
  + Возможность масштабирования Системы, наращивания её производительности, устойчивую работу Системы в условиях увеличения объемов хранимых данных прикладных систем и задач;
  + Совместимость компонентов системы на аппаратном уровне и на уровнях операционных систем и базовых программных средств;
  + Применимость решения по созданию системы к существующим серверным платформам и операционным средам;
  + Поставляемая аппаратная платформа должна соответствовать требованиям производителей программного обеспечения. Производитель программного обеспечения обязан гарантировать поддержку Системы на поставляемой аппаратной платформе.

1. Содержание выполняемых Работ и оказываемых Услуг

**Работы по созданию Системы включают следующие этапы:**

**Этап 1. Проектирование.**

На данном этапе производится:

* обследование инфраструктуры Заказчика, выявление текущих потребностей по защите информации от утечек;
* подготовка технических требований к площадкам для внедрения Системы;
* сбор информации по настройке политик и правил реакции системы при мониторинге различного рода информации, подготовка описания правил и политик;
* разработка документации на Систему, указанной в п.7.;

**Этап 2. Запуск и сопровождение опытной эксплуатации Системы.**

На данном этапе производится:

* производится поставка лицензий Системы на 50 (Пятьдесят) рабочих мест;
* монтаж и пуско-наладочные работы программно-аппаратных составляющих Системы;
* проводятся предварительные испытания Системы;
* проверка корректности функционирования Системы в инфраструктуре Заказчика,
* настройка правил и политик реакции Системы на анализируемые события,
* настройка классификатора по требованиям защиты информации Заказчика в соответствии с отраслевыми требованиями;
* прохождение программы методик испытания;
* обучение специалистов Заказчика по курсам Офицер безопасности и Специалист по сопровождению и администрированию.

**Этап 3. Запуск промышленной эксплуатации Системы.**

На данном этапе производится:

* поставка лицензий Системы на 150 (Сто пятьдесят) рабочих мест;
* монтаж и пусконаладка программно-аппаратных составляющих системы;
* установка системы на удаленных площадках;
* предварительные испытания Системы;
* проверка корректности функционирования Системы в инфраструктуре Заказчика,
* настройка правил и политик реакции Системы на анализируемые события;
* настройка классификатора по требованиям защиты информации Заказчика в соответствии с отраслевыми требованиями;
* прохождение программы методик испытания.

**Услуги по технической поддержке Системы включают:**

* Консультации работников Заказчика по телефону и электронной почте с 10:00 до 18:00 по московскому времени в рабочие дни.
* Оказание консультационной и технической помощи специалистам, обслуживающим Систему, по вопросам ее функционирования, эксплуатации, диагностики неисправностей и проведения восстановительных работ по телефону, факсу и электронной почте. При этом должны соблюдаться следующие требования:

время первичной реакции на запрос Заказчика – не более 30 минут;

время выполнения запроса с высоким приоритетом (инцидент влияет на функционал системы и приводит к ее неработоспособности) – не более 4 часов;

время выполнения запроса с средним приоритетом Средний (инцидент влияет на функционал системы, но не приводит к ее неработоспособности) – не более 8 часов;

время выполнения запроса с низким приоритетом (консультации по функционалу системы, работоспособность системы не нарушена) – не более 20 часов.

* Предоставление выпускаемых обновлений программного обеспечения компонентов Системы.

1. Порядок проведения испытаний Системы
   1. Общие требования к испытаниям Системы
      1. Предварительные испытания Системы проводятся представителями Исполнителя с участием представителей Заказчика.
      2. Опытная эксплуатация проводится представителями Заказчика после проведения предварительных испытаний и подписания Сторонами Акта о переводе системы в опытно-промышленную эксплуатацию.
      3. Представители Исполнителя перед началом опытной эксплуатации проводят краткое обучение навыкам работы с Системой, и в дальнейшем наблюдают за ходом испытаний, консультируют представителей Заказчика по вопросам работы с Системой, участвуют в процессе сбора и формализации дополнительных требований по защиты информации полученных от Заказчика, проводят интервьюирования с представителями Заказчика, выполняют донастройку Системы по формализованным требованиям.
      4. Приемочные испытания Системы проводятся представителями Исполнителя с участием представителей Заказчика.
2. Требования к оформлению документов, предоставляемых в ходе (по итогам) выполнения Работ
   1. В ходы выполнения Работ Исполнитель должен подготовить следующие документы, которые делятся на два вида:

* Рабочая документация;
* Эксплуатационная документация.
  1. Рабочая документация включает в себя:
* Пояснительная записка к техническому проекту.
* Описание Базы контентной фильтрации.
* Методика проведения расследований инцидентов.
* Программа и методика предварительных испытаний.
* Протокол предварительных испытаний.
* Акт о передаче Системы в опытную эксплуатацию.
* Программа опытной эксплуатации.
* Журнал опытной эксплуатации.
* Акт о завершении опытной эксплуатации и допуске системы к приемочным испытаниям.
* Программа и методика приемочных испытаний.
* Протокол приемочных испытаний.
* Акт о передаче Системы Заказчику для ввода в промышленную эксплуатацию.
  1. Эксплуатационная документация включает в себя:
* Инструкция администратора Системы;
* Инструкция пользователя;
* Паспорт Системы.
  1. По результатам выполнения Работ Исполнитель представляет материалы, указанные в пп.7.2-7.3 раздела 7 настоящего документа.
  2. Вся разрабатываемая документация должна соответствовать действующим нормам и стандартам, включая положения ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем».
  3. Вся перечисленная выше документация передается Заказчику на бумажном носителе в 2 (двух) экземплярах и в электронном виде на диске CD (DVD) в 1 (одном) экземпляре и должна быть выполнена на русском языке.
  4. Документация в электронном виде предоставляется Заказчику в формате:
* текстовые документы - Microsoft Word (либо PDF);
* схемы, рисунки и другие графические материалы - Microsoft Visio (либо PDF).

1. Состав Работ
   1. Работы проводятся в соответствии с календарным планом-графиком, согласованным с Заказчиком.
   2. Состав и содержание Работ приведены в таблице №1.

**Таблица №1**

| **№ п/п** | **Состав и содержание работ** | **Результат (индикатор) выполнения работ** |
| --- | --- | --- |
| **Этап 1. Проектирование** | | |
| 1.1 | Обследование объектов автоматизации | * + - Собраны количественные данные об объемах трафика;     - Собраны данные о смежных системах;     - Получена схема сети;     - Получены документы с описаниями политик безопасности; |
| 1.2 | Разработка документации на Систему | Разработаны и переданы Заказчику документы:   * + - План мероприятий по подготовке площадки;     - Пояснительная записка к Техническому проекту;     - Методика проведения расследований инцидентов;     - Программа опытной эксплуатации;     - Программа и методика приемочных испытаний Системы;     - Инструкция администратора;     - Инструкция пользователя;     - Паспорт Системы; |
| **Этап 2. Опытная эксплуатация** | | |
| 2.1 | Поставка лицензий | * + - Лицензии поставлены; |
| 2.2 | Установка и настройка серверного и клиентского программного обеспечения, интеграция со смежными системами | * + - Проведена установка ПО;     - Проведена настройка ПО в соответствии с ПЗ;     - Проведена интеграция со смежными системами в соответствии с ПЗ; |
| 2.3. | Проведение предварительных испытаний | * + - Предварительные испытания проведены, система допущена в опытную эксплуатацию; |
| 2.4. | Обучение | * + - Проведено обучение специалистов Заказчика; |
| 2.5. | Опытная эксплуатация | * + - Зафиксированы замечания к системе в журнале опытной эксплуатации;     - Устранены замечания, выявленные в ходе опытной эксплуатации; |
| 2.6. | Проведение приемочных испытаний | * + - Приемочные испытания проведены, система допущена в опытно-промышленную эксплуатацию;     - Подписан Акт о переводе системы в опытно-промышленную эксплуатацию; |
| **Этап 3. Промышленная эксплуатация** | | |
| 3.1. | Поставка лицензий | * + - Лицензии поставлены; |
| 3.2. | Установка и настройка серверного и клиентского программного обеспечения, интеграция со смежными системами | * + - Проведена установка ПО;     - Проведена настройка ПО в соответствии с ПЗ;     - Проведена интеграция со смежными системами в соответствии с ПЗ; |
| 3.3. | Проведение приемочных испытаний | * + - Проведены приемочные испытания Системы;     - Подписан Акт сдачи-приемки выполненных Работ |

Исполнитель в своём Техническом предложении должен определить сроки выполнения Работ.

1. Иные требования
   1. До начала работ Заказчик и Исполнитель должны:

* назначить Ответственного представителя (от Заказчика) и Руководителя работ (от Исполнителя), которые уполномочены оперативно решать все организационные и технические вопросы при выполнении и сдаче-приемке выполненных работ;
* подписать соглашение о неразглашении конфиденциальной информации;
* перед началом очередной стадии работ по проекту согласовать детальный график работ;
* согласовать порядок входа на объект и режим пребывания специалистов Исполнителя на объекте в течение рабочего дня, а при необходимости, также в вечернее время и в выходные дни;
* для своевременного контроля над ходом проведения работ согласовать порядок предоставления Заказчику отчетов о выполненных и проводимых работах;
* согласовать порядок сдачи выполненных монтажных работ и проведения приемо-сдаточных испытаний.
  1. Требования к подготовке исходных данных

Для разработки документации Заказчик должен предоставить Исполнителю все необходимые для проведения работ исходные данные, в том числе:

* информацию о серверах и рабочих станциях, функционирующих в компании предназначенных для развертывания Системы;
* информацию о существующей системе управления настройками серверов и рабочих станций и правами пользователей.

Получение любой информации от работников Заказчика, необходимой для выполнения проекта, должно осуществляться Исполнителем в режиме интервьюирования (с оформлением результатов в письменном виде силами Исполнителя и согласованием с Заказчиком).

Перечень исходных данных уточняется и дополняется в ходе выполнения работ установленным порядком.

* 1. Требования к сети электропитания
     1. Поставляемое оборудование должно быть рассчитано на питание от сети переменного тока 220 Вольт, частотой 50 Гц, перерывы питания в сети не допускаются, допускаются колебания напряжения не более 5%, колебания частоты не более 1%.
     2. Наличие в помещении электрораспределительного щита, оснащенного автоматическими пакетными переключателями (предохранителями).
     3. Электроснабжение помещения с телекоммуникационным оборудованием должно относиться к группе 1 категории ПЭУ.
     4. Помещения с телекоммуникационным оборудованием должны быть оборудованы защитным заземлением в соответствии с ГОСТ 464-79 и устройствами молниезащиты.

Приложение 1

к Техническому заданию

**Спецификация**

|  |  |  |
| --- | --- | --- |
| **№** | **Описание** | **Кол-во ПК** |
| 1. | Лицензия на право использования программного обеспечения InfoWatch Traffic Monitor 500 / License for InfoWatch Traffic Monitor 500 | 200 |
|  | В составе:   * компонент программного обеспечения InfoWatch Traffic Monitor: InfoWatch Traffic Monitor Base выпуск с полным комплектом модулей анализа / License for the InfoWatch Traffic Monitor software component: InfoWatch Traffic Monitor Base release with all analysis modules * компонент программного обеспечения InfoWatch Traffic Monitor: InfoWatch Traffic Monitor for HTTPS / License for the InfoWatch Traffic Monitor software component: InfoWatch Traffic Monitor for HTTPS * компонент программного обеспечения InfoWatch Traffic Monitor: InfoWatch Crawler / License for the InfoWatch Traffic Monitor software component: InfoWatch Crawler * компонент программного обеспечения InfoWatch Traffic Monitor: InfoWatch Traffic Monitor (полный комплект перехватчиков) / License for the InfoWatch Traffic Monitor software component: InfoWatch Traffic Monitor (all interceptors) * компонент программного обеспечения InfoWatch Traffic Monitor: InfoWatch OCR module / License for the InfoWatch Traffic Monitor software component: InfoWatch OCR module |  |
| 2. | Техническая поддержка программного обеспечения InfoWatch Traffic Monitor 500 | 200 |

|  |  |
| --- | --- |
| **ЗАКАЗЧИК:** | **ИСПОЛНИТЕЛЬ:** |