**Протокол № ЗК-ДБ-191/2**

**рассмотрения и оценки котировочных заявок**

**(ОАО «КСК»)**

|  |  |
| --- | --- |
| **г. Москва** | **23 сентября 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, Гарага Дмитрий Сергеевич, Дубенко Павел Николаевич, Зверева Наталья Алексеевна, Иванов Николай Васильевич, Канукоев Аслан Султанович, Кузнецов Андрей Александрович, Чернышев Юрий Александрович, Голосов Дмитрий Александрович.

На заседание Единой комиссии в качестве эксперта приглашен: эксперт отдела корпоративной защиты и информационной безопасности – Неруш Сергей Григорьевич.

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 20:00 (мск) 27 августа 2014 года № ЗК-ДБ-191.
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** | 2 597 530,00 (Два миллиона пятьсот девяносто семь тысяч пятьсот тридцать) рублей 00 копеек, без учета НДС.  В цену договора включены все расходы поставщика услуг на уплату сборов, налогов (помимо НДС) и иных обязательных платежей. |
| **Наименование, перечень выполняемых работ/оказываемых услуг** | 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** | 455 (Четыреста пятьдесят пять) календарных дней со дня заключения договора.  Срок выполнения работ по созданию автоматизированной системы защиты конфиденциальной информации с предоставлением Заказчику необходимой простой (неисключительной) лицензии на программное обеспечение – 90 (Девяносто) календарных дней со дня заключения Договора.  Срок оказания услуг оказание услуг по технической поддержке автоматизированной системы защиты конфиденциальной информации – 1 (Один) год с даты приемки Заказчиков результата работ по ее созданию. |
| **Финансирование** | Собственные средства ОАО «КСК». |

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

| **Регистрационный номер заявки участника закупки** | **Наименование участника закупки** | **Юридический/почтовый адреса участника закупки** |
| --- | --- | --- |
| № 301  от 04 сентября 2014 года 15:30 (мск) | **ОАО «МТТ»**  (ИНН 7705017253) | Юридический адрес / почтовый адрес:  109147, г. Москва, ул. Маркситская,  д. 22, стр. 1  Тел.: 8-499-709-01-01 |
| № 302  от 04 сентября 2014 года 15:40 (мск) | **ЗАО «КРОК инкорпорейтед»**  (ИНН 7701004101) | Юридический адрес:  105082, г. Москва, ул. Большая Почтовая, д. 26В, стр. 2  Почтовый адрес:  111033, г. Москва, ул. Волочаевская, д. 5, к. 1  Тел.:8-495-974-22-74 |
| № 304  от 15 сентября 2014 года 11:30 (мск) | **ОАО «АйСиЭл-**  **КПО ВС»**  (ИНН 1660014361) | Юридический адрес / почтовый адрес:  420029, г. Казань, ул. Сибирский тракт, д. 34  Тел.: 8-843-567-57-57 |
| № 305  от 16 сентября 2014 года 12:10 (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. 2  Тел.:8-495-280-15-50 |

1. Результаты рассмотрения котировочных заявок на соответствие их требованиям, установленным в запросе котировок (Извещение от 27 августа 2014 года № ЗК-ДБ-191):
   1. Участник закупки **ОАО «МТТ»** (ИНН 7705017253) не соответствует требованиям:

|  |  |  |
| --- | --- | --- |
| **№** | **Требование** | **Несоответствие** |
| 1. | 2.2. Участник закупки должен иметь партнерский статус с компанией InfoWatch, что подтверждается предоставлением Авторизационного письма от компании – разработчика, подготовленного в адрес ОАО «КСК» (подтверждается предоставлением копии авторизационного письма от компании InfoWatch). | Копия письма не представлена. |
| 2. | 2.3. Участник закупки должен быть авторизованным партнером по оказанию сервисных услуг InfoWatch Solution Provider (подтверждается предоставлением копии авторизационного письма от компании InfoWatch). | Копия письма не представлена. |
| 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 предоставлением копий сертификатов);  • не менее 1 (одного) специалиста по управлению проектами Project Management Professional или Project Management Expert (PMP/PME) (подтверждается предоставлением копий сертификатов). | Копии сертификатов не представлены. |
| 4. | Участник закупки должен иметь действующий сертификат соответствия системы менеджмента качества, разработанной на основании требований, установленных стандартом ГОСТ Р ИСО 9001-2008 «Система менеджмента качества. Требования» (подтверждается предоставлением копии сертификата). | Копия сертификата не представлена. |

Приглашенный эксперт (С.Г. Неруш) подтверждает несоответствие требованиям, указанным в Извещении от 27 августа 2014 года № ЗК-ДБ-191.

* 1. Участник закупки **ЗАО «КРОК инкорпорейтед»** (ИНН 7701004101) не соответствует требованиям:

|  |  |  |
| --- | --- | --- |
| **№** | **Требование** | **Несоответствие** |
| 1. | Превышение участником закупки начальной (максимальной) цены договора, установленной Извещением о проведении запроса котировок. | Участником закупки предложена цена договора 2 923 728,81 (Два миллиона девятьсот двадцать три тысячи семьсот двадцать восемь) рублей 81 копейка, без учета НДС. |

Приглашенный эксперт (С.Г. Неруш) подтверждает несоответствие требованиям, указанным в Извещении от 27 августа 2014 года № ЗК-ДБ-191.

* 1. Участник закупки **ОАО «АйСиЭл-КПО ВС»** (ИНН 1660014361) не соответствует требованиям:

|  |  |  |
| --- | --- | --- |
| **№** | **Требование** | **Несоответствие** |
| 1. | 2.1. Наличие у участника закупки Лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации (подтверждается предоставлением копии лицензии). | В представленной копии лицензии указан срок действия до 07 сентября 2014 года. |
| 2. | 2.2. Участник закупки должен иметь партнерский статус с компанией InfoWatch, что подтверждается предоставлением Авторизационного письма от компании – разработчика, подготовленного в адрес ОАО «КСК» (подтверждается предоставлением копии авторизационного письма от компании InfoWatch). | Копия письма не представлена. |
| 3. | 2.3. Участник закупки должен быть авторизованным партнером по оказанию сервисных услуг InfoWatch Solution Provider (подтверждается предоставлением копии авторизационного письма от компании InfoWatch). | Копия письма не представлена. |

Приглашенный эксперт (С.Г. Неруш) подтверждает несоответствие требованиям, указанным в Извещении от 27 августа 2014 года № ЗК-ДБ-191.

* 1. Участник закупки **ЗАО «Андэк»** (ИНН 7726585419) соответствует требованиям, указанным в Извещении от 27 августа 2014 года № ЗК-ДБ-191.

Приглашенный эксперт (С.Г. Неруш) подтверждает соответствие требованиям, указанным в Извещении от 27 августа 2014 года № ЗК-ДБ-191.

1. **Решение:**
   1. В соответствии с п. 17.19 «Положения о закупке товаров, работ, услуг   
      для нужд ОАО «КСК», признать запрос котировок (Извещение от 27 августа 2014 года № ЗК-ДБ-191) 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 «Андэк»**(ИНН 7726585419), с ценой договора **2 450 000** (Два миллиона четыреста пятьдесят тысяч) рублей, без учета НДС.

**Результат голосования:**

**«За» - 5 голосов:**

Гарага Дмитрий Сергеевич;

Дубенко Павел Николаевич;

Иванов Николай Васильевич;

Канукоев Аслан Султанович;

Кузнецов Андрей Александрович.

**«Против» - 1 голос:**

Шашкин Никита Артемович.

**«Воздержалось» - 3 голоса:**

Горчев Олег Сергеевич;

Зверева Наталья Алексеевна;

Чернышев Юрий Александрович.

**Решение принято большинством голосов.**

* 1. Настоящий протокол подлежит хранению не менее трех лет.

**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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гарага Дмитрий Сергеевич

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

Член комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Зверева Наталья Алексеевна

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

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

Член комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Кузнецов Андрей Александрович

Член комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Чернышев Юрий Александрович

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

Эксперт \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Неруш Сергей Григорьевич

**Приложение № 1 к Протоколу  
от 23 сентября 2014 года № ЗК**-**ДБ-191/2**

**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.
   2. Исполнитель должен создать систему защиты информации от внутренних угроз и утечек конфиденциальных данных (далее – Система) в ОАО «КСК» в объеме, предусмотренном настоящим Техническим заданием, и осуществлять техническую поддержку Системы на протяжении одного года на условиях Договора.
2. **Назначение и цели создания Системы**
   1. Целью создания автоматизированной системы защиты конфиденциальной информации является обеспечение информационной безопасности Заказчика 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 следующих процессов:

* 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 одновременно обслуживаемых (защищаемых) Программным обеспечением рабочих станций (ЭВМ) – 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. Система должна функционировать в составе распределенной информационно-вычислительной сети;
      3. Система должна функционировать по клиент-серверной схеме;
      4. Система должна функционировать при установке на терминальных рабочих станциях, созданных на базе продукта Microsoft Terminal Services;
      5. Система должна обладать возможностью масштабирования;
      6. Система должна 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;
      7. Система должна обеспечивать возможность интеграции со следующими proxy-серверами: Squid, Cisco IronPort, Bluecoat ProxySG, Microsoft Forefront TMG;
      8. Система должна обеспечивать возможность интеграции со следующими смежными продуктами: DeviceLock, Microsoft Lync Server 2010, Microsoft Exchange Server, ArcSight;
      9. Система должна обеспечивать возможность интеграции и идентификации объектов с данными, полученными из Active Directory;
      10. Система должна быть спроектирована для возможного использования в структуре филиалов, соединенных любыми поддерживаемыми совместимыми операционными системами каналами связи, в том числе с низкой пропускной способностью (от 2Мбит\с);
      11. Для информационного обмена между компонентами системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP;
      12. Система должна обеспечивать возможность контроля трафика удаленных элементов информационной системы.
      13. 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:
* Система должна обеспечивать возможность записи в журналы аудита информации по служебным событиям и сбоям. Записи в журналах должны содержать информацию, достаточную для установления причины неисправности;
* Система должна обеспечивать штатное функционирование в случае одновременной работы всех пользователей на объекте автоматизации;
* Система должна быть способна 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: съемные носители, 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, изображения emf;
* 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 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, предусмотренной к разработке Таблицей № 1 настоящего Технического задания;

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

На данном этапе производится:

* производится поставка Лицензии Системы на 200 (Двести) ЭВМ площадки в г. Москве и в г. Пятигорске;
* монтаж и пуско-наладочные работы программно-аппаратных составляющих Системы;
* проводятся предварительные испытания Системы на площадке в г. Москве;
* проверка корректности функционирования Системы в инфраструктуре Заказчика,
* настройка правил и политик реакции Системы на анализируемые события;
* настройка классификатора по требованиям защиты информации Заказчика;
* проведение опытной эксплуатации;
* обучение специалистов Заказчика по курсам «Офицер безопасности» и «Специалист по сопровождению и администрированию».

**Этап 3. Запуск промышленной эксплуатации Системы**

На данном этапе производится:

* монтаж и пуско-наладка программно-аппаратных составляющих системы;
* установка системы на удаленной площадке;
* проверка корректности функционирования Системы в инфраструктуре Заказчика,
* настройка правил и политик реакции Системы на анализируемые события;
* настройка классификатора по требованиям защиты информации Заказчика;
* прохождение приемочных испытаний.

Условия оказания услуг по технической поддержке Системы описаны в Соглашении об уровне обслуживания (Приложение № 5 к Договору).

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 и по итогам выполнения Работ**
   1. В ходе выполнения Работ Исполнитель должен подготовить следующие документы, которые делятся на два вида:

* Проектно-рабочая документация;
* Эксплуатационная документация.
  1. Проектно-рабочая документация включает в себя:
* Пояснительная записка к техническому проекту;
* План мероприятий по подготовке площадки;
* Описание Базы контентной фильтрации. Программа и методика испытаний. Документ должен описывать программу и методику испытаний для предварительных и приемочных 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;
* Протокол приемочных испытаний;
* Акт о передаче Системы Заказчику для ввода в промышленную эксплуатацию.
  1. Эксплуатационная документация включает в себя:
* Инструкция администратора Системы;
* Инструкция пользователя;
* Методика проведения расследований инцидентов;
* Паспорт Системы.
  1. По результатам выполнения Работ Исполнитель представляет Заказчику материалы, указанные в п.п. 7.2-7.3 раздела 8 настоящего Технического задания.
  2. Вся перечисленная выше документация передается Заказчику в электронном виде на электронном носителе информации в одном экземпляре и должна быть выполнена на русском языке.
  3. 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 (далее - ПЗ);     - Методика проведения расследований инцидентов;     - Программа опытной эксплуатации;     - Программа и методика испытаний Системы;     - Инструкция администратора;     - Инструкция пользователя;     - Описание Базы контентной фильтрации;     - Паспорт Системы. |
| **Этап 2. Опытная эксплуатация** | | |
| 2.1 | Установка и настройка серверного и клиентского программного обеспечения, интеграция со смежными системами (г. Москва) | * + - Заказчику передана лицензия для использования Программного обеспечения (далее - ПО) на 200 (Двухстах) ЭВМ одновременно;     - Проведена установка ПО;     - Проведена настройка ПО в соответствии с ПЗ;     - Проведена интеграция со смежными системами в соответствии с ПЗ. |
| 2.2. | Проведение предварительных испытаний | * + - Предварительные испытания проведены, система допущена в опытную эксплуатацию;     - Протокол предварительных испытаний. |
| 2.3. | Обучение | * + - Проведено обучение специалистов Заказчика. |
| 2.4. | Опытная эксплуатация | * + - Зафиксированы замечания к системе в журнале опытной эксплуатации;     - Устранены замечания, выявленные в ходе опытной эксплуатации. |
| **Этап 3. Промышленная эксплуатация** | | |
| 3.1. | 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. |
| 3.2. | Проведение приемочных испытаний | * + - Проведены приемочные испытания Системы;     - Подписан Акт сдачи-приемки выполненных Работ. |

Начало обучения специалистов Заказчика (п. 2.3 Таблицы № 1) по согласованию с Заказчиком может быть начато Исполнителем на более ранней стадии исполнения Договора.

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), либо в электронном виде.

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

* 1. Заказчик после получения от Исполнителя Плана мероприятий по подготовке площадки проводит работы по обеспечению готовности площадки к внедрению Системы.

Приложение 1

к Техническому заданию

Спецификация внедряемого в рамках Договора Программного обеспечения

Программноe обеспечение InfoWatch Traffic Monitor 500 в составе:

• компонент программного обеспечения InfoWatch Traffic Monitor: InfoWatch Traffic Monitor Base выпуск с полным комплектом модулей анализа / 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 / InfoWatch Traffic Monitor software component: InfoWatch Traffic Monitor for HTTPS;

• компонент программного обеспечения InfoWatch Traffic Monitor: InfoWatch Crawler / InfoWatch Traffic Monitor software component: InfoWatch Crawler;

• компонент программного обеспечения InfoWatch Traffic Monitor: InfoWatch Traffic Monitor (полный комплект перехватчиков) / InfoWatch Traffic Monitor software component: InfoWatch Traffic Monitor (all interceptors);

• компонент программного обеспечения InfoWatch Traffic Monitor: InfoWatch OCR module / InfoWatch Traffic Monitor software component: InfoWatch OCR module.

Количество рабочих станций (ЭВМ), на которых Программное обеспечение может одновременно использоваться при исполнении Договора, - 200 (Двести) шт.

Приложение 2

к Техническому заданию

Состав передаваемой по Договору Лицензии

|  |  |  |
| --- | --- | --- |
| № | Наименование ограниченных прав на использование программ для ЭВМ (простой (неисключительной) лицензии) | Кол-во ЭВМ, шт. |
| 1 | Лицензия на право использования программного обеспечения InfoWatch Traffic Monitor 500 / License for InfoWatch Traffic Monitor 500 в составе:   * лицензия на право использования компонента 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; * лицензия на право использования компонента программного обеспечения InfoWatch Traffic Monitor: InfoWatch Traffic Monitor for HTTPS / License for the InfoWatch Traffic Monitor software component: InfoWatch Traffic Monitor for HTTPS; * лицензия на право использования компонента программного обеспечения InfoWatch Traffic Monitor: InfoWatch Crawler / License for the InfoWatch Traffic Monitor software component: InfoWatch Crawler; * лицензия на право использования компонента программного обеспечения InfoWatch Traffic Monitor: InfoWatch Traffic Monitor (полный комплект перехватчиков) / License for the InfoWatch Traffic Monitor software component: InfoWatch Traffic Monitor (all interceptors); * лицензия на право использования компонента программного обеспечения InfoWatch Traffic Monitor: InfoWatch OCR module / License for the InfoWatch Traffic Monitor software component: InfoWatch OCR module. | 200 |