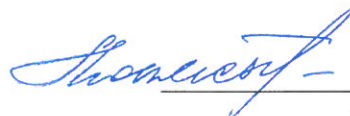


Приложение № 1
к запросу коммерческого предложения

УТВЕРЖДАЮ

Заместитель генерального
директора по безопасности
АО «НоваВинд»



Ю.А. Токмачев
«22» октября 2019

Техническое задание

Предмет закупки: предоставление права использования программного обеспечения и оказание услуг по техническому внедрению

Москва
2019

СОДЕРЖАНИЕ

РАЗДЕЛ 1. НАИМЕНОВАНИЕ УСЛУГИ

РАЗДЕЛ 2. ОПИСАНИЕ УСЛУГ

Подраздел 2.1 Состав (перечень) оказываемых услуг

Подраздел 2.2 Описание оказываемых услуг

Подраздел 2.3 Объем оказываемых услуг либо доля оказываемых услуг
в общем объеме закупки

РАЗДЕЛ 3. ТРЕБОВАНИЯ К УСЛУГАМ

Подраздел 3.1 Общие требования

Подраздел 3.2 Требования к качеству оказываемых услуг

Подраздел 3.3 Требования к гарантийным обязательствам оказываемых
услуг

Подраздел 3.4 Требования к конфиденциальности

Подраздел 3.5 Требования к безопасности оказания услуг и
безопасности результата оказанных услуг

Подраздел 3.6 Специальные требования

РАЗДЕЛ 4. РЕЗУЛЬТАТ ОКАЗАННЫХ УСЛУГ

Подраздел 4.1 Описание конечного результата оказанных услуг

Подраздел 4.2 Требования по приемке услуг

Подраздел 4.3 Требования по передаче сублицензиату технических и
иных документов (оформление результатов оказанных услуг)

РАЗДЕЛ 5. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБУЧЕНИЮ ПЕРСОНАЛА СУБЛИЦЕНЗИАТА

РАЗДЕЛ 6. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

РАЗДЕЛ 7. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ

РАЗДЕЛ 1. НАИМЕНОВАНИЕ ПРЕДМЕТА ЗАКУПКИ

Предоставление права использования программного обеспечения, оказание услуг по техническому внедрению и поставка сертификата на услуги по технической поддержке и сопровождению программного обеспечения.

РАЗДЕЛ 2. ОПИСАНИЕ ПРАВА ИСПОЛЬЗОВАНИЯ РИД, УСЛУГИ

Подраздел 2.1 Состав (перечень) оказываемых услуг, прав использования РИД

2.1.1. предоставление права использования информационно-аналитической системы контент-мониторинга информационных потоков и действий сотрудников Сублицензиата в части обращения с информацией ограниченного доступа, **включая информацию, относящуюся к интеллектуальной собственности технологического партнера - компании Lagerway Systems B.V. (Нидерланды)** (далее конфиденциальная информация - КИ), далее в целом – «Система».

2.1.2. Услуги по техническому внедрению Системы на оборудование Сублицензиата силами специалистов Лицензиата.

2.1.3. Поставка сертификата на услуги по технической поддержке и сопровождению ПО в количестве 1 шт.

Конечным пользователем по данному сертификату должен являться АО «НоваВинд».

Сертификат должен быть поставлен в течении 5 рабочих дней с даты подписания сублицензионного договора.

Подраздел 2.2. Описание предоставления права использования РИД, оказания услуг

2.2.1. Лицензиат предоставляет Сублицензиату право использования программного обеспечения (далее – ПО) в количестве одна сетевая лицензия с количеством обслуживаемых учетных записей пользователей не менее 300. Передача права использования ПО осуществляется на материальном носителе информации. Целями оказания услуг являются получение Сублицензиатом настроенной в соответствии с данным техническим заданием Системы.

Система предоставляется на срок 3 года с даты подписания Сторонами Акта приема-передачи прав и должна обеспечивать реализацию функционала:

- Контроль на конечных узлах в виде аудита или блокировки транзакций с КИ по каналам:
 - Removable (отправка на USB носители)
 - Endpoint LAN (Сохранение на Сетевые каталоги)
 - Printing (Печать)
 - Application Control (Контроль приложений)
 - Endpoint Email (Контроль Outlook)

- Endpoint Discovery (Обнаружение КИ на узлах)
- Контроль веб трафика по каналам HTTP/HTTPS с помощью Веб шлюза:
 - URL Фильтрация по объектам из Active Directory
 - Аудит или блокирование транзакций с КИ
 - Антивирусная защита
 - Отказоустойчивость при доступе к ресурсам Интернет
- количество обслуживаемых учетных записей пользователей – 300 с перспективой расширения до 500 в течение 3 лет.
- производительность Системы должна быть достаточной для обеспечения:
 - в подсистеме контент-мониторинга до 500 пользователей,
 - в подсистеме повышения и проверки уровня осведомленности – не более 500 при количестве одновременно работающих пользователей с порталом обучения – не более 100. Длительность формирования отчета не более 200 секунд.

2.2.2. Услуги по техническому внедрению Системы на оборудование Сублицензиата силами специалистов Лицензиата должны включать в себя:

Установку Системы на оборудовании Сублицензиата силами специалистов Лицензиата. После установки компонентов Системы должна быть произведена её пуско-наладка, первичная настройка политик Системы и интеграция Системы с корпоративными ИТ-сервисами организации Сублицензиата (где это возможно и необходимо для соответствия требованиям настоящего ТЗ).

Со стороны Лицензиата должно быть предусмотрено выполнение нижеследующих объёмов работ, путем непосредственного их проведения силами специалистов и инженеров Лицензиата в офисе Сублицензиата (дистанционные работы не допустимы):

- обследование и анализ инфраструктуры Сублицензиата, для подготовки архитектуры внедрения;
- размещение компонентов в инфраструктуре Сублицензиата;
- установка Системы;
- первичная настройка политик Системы;
- интеграция Системы с корпоративными сервисами Сублицензиата;
- настройка отказоустойчивого режима работы;
- проверка отказоустойчивости и корректной отработки оповещений системы мониторинга
- настройка правил контент- мониторинга (Лицензиатом должна быть настроена базовая политика контент-мониторинга;
- настройка подсистемы оповещения об инцидентах;
- развертывание подсистемы оптического распознавания символов (OCR) и интеграция с Веб шлюзом для анализа наличия КИ в графических файлах;
- развертывание системы централизованного управления компонентами Системы;

- развертывание и настройка кластеризации Веб шлюза для отказоустойчивости работы;
- настройка на Веб шлюзе интеграции с Active Directory для разграничения и фильтрации пользовательского доступа к ресурсам Интернет;
- настройка на Веб шлюзе аутентификации Kerberos;
- настройка на Веб шлюзе интеграцию с DLP модулем и HTTPS инспекцию;
- настройка правил доступа в Интернет для базового набора групп пользователей в соответствии с пожеланиями Сублицензиата;
- настройка защитных механизмов в соответствии с базовой настройкой. Правила защитных механизмов предполагающие различные варианты настроек необходимо настроить по согласованию с Сублицензиатом;
- установка Агентов на базовой (пилотной) группе рабочих мест пользователей и помощь в последующем тиражировании установки Агентов на машины сотрудников компании Сублицензиата.

2.2.3. Сертификат на услуги по технической поддержке и сопровождению ПО включает в себя:

- возможность обращения в службу технической поддержки по приобретаемому ПО, в соответствии со стандартным соглашением об уровне сервиса (SLA) на РТП;
- разрешение инцидентов/проблем (работа по запросам), относящихся к стандартной функциональности приобретаемого ПО (включая новые версии, сервисные пакеты и исправления), связанных с установкой, настройкой и эксплуатацией;
- консультации по технической поддержке ПО.

Подраздел 2.3. Объем оказываемых услуг либо доля оказываемых услуг в общем объеме закупки

Система должна работать (включая необходимое обеспечение неисключительными правами на использование ПО) не менее 3 лет (36 месяцев).

Количество обслуживаемых учетных записей пользователей - не менее 300.

РАЗДЕЛ 3. ТРЕБОВАНИЯ К УСЛУГАМ

Подраздел 3.1. Общие требования

3.1.1. Срок действия прав на использование ПО: не менее 3 лет (36 месяцев) с даты подписания Сторонами Акта приема-передачи прав.

3.1.2. Система должна соответствовать разделу 2.2. настоящего Технического задания.

3.1.3. Предоставляемое право использования ПО должно включать в себя следующие способы:

- воспроизведение ПО путем записи его в память ЭВМ, ограниченное

правом инсталляции, копирования и запуска программ для ЭВМ в количестве 1 экземпляра;

- совершение любых действий, связанных с функционированием программы в соответствии с ее назначением и документацией во внутрипроизводственной деятельности Сублицензиата.

3.1.4. Лицензиат в течение 3 рабочих дней с даты заключения договора передает Сублицензиату права на использование ПО, путем предоставления ПО на материальном носителе.

3.1.5. Услуги по техническому внедрению Системы на оборудование Сублицензиата должны быть оказаны в полном объеме в течении 5 рабочих дней с даты подписания сублицензионного договора.

По результатам оказанных услуг Сублицензиат должен иметь внедренную Систему по установленному настоящим ТЗ функционалу.

Услуги оказываются по месту нахождения Сублицензиата: г. Москва, л. Щипок, д. 18, стр.2.

3.1.6. После внедрения Система должна функционировать непрерывно и круглосуточно (24/7). Под непрерывным режимом работы Системы понимается режим работы, при котором Система постоянно находится в рабочем состоянии (выполняют свои функции), за исключением времени, необходимого для его планового и внепланового технического обслуживания. ПО должно поддерживать многопользовательский режим работы.

3.1.7. Доступность инженеров технической поддержки, как в рабочие, так и в выходные дни (суббота и воскресенье) с 08:00 до 19:00 по Московскому времени (GMT +3).

Подраздел 3.2. Требования к качеству оказываемых услуг

Внедряемая Система должна быть интегрирована в общий контур системы обеспечения информационной безопасности Сублицензиата.

Для обеспечения безопасности в Системе используются следующие меры:

- хранение всех данных на сервере;
- присвоение каждому Администратору логина и пароля для доступа в Систему;
- задание уровней доступа для различных категорий Администраторов Системы;
- разграничение прав доступа для отдельных групп и категорий Администраторов Системы, в частности, по ролям и уровням доступа.

Контент-мониторинг входящего интернет-трафика (далее - Веб-шлюз)

• Веб шлюз должен обеспечивать проксирование соединений по протоколам HTTP, HTTPS, FTP с кэш-памятью

• Прокси-аутентификация пользователей с помощью Kerberos, NTLM, LDAP или клиентских сертификатов, настройка в виде наборов правил

• Работа в режиме явного или прозрачного прокси-сервера с

поддержкой протокола WCCP

- Поддержка кластерных режимов для отказоустойчивости и виртуальной адресации IP
- Скоростное инспектирование значительной доли трафика HTTPS с механизмами исключений по адресам или категориям веб-сайтов
- Прозрачная идентификация пользователей Active Directory по адресам IP с использованием как собственной инфраструктуры Active Directory, так и совместимых систем
- Тематическая фильтрация веб-сайтов по адресам URL с использованием регулярно обновляемой базы
- Поддержка национальных доменных имён (IDN), фильтрация имён в зоне «.рф»
- Программируемый интерфейс приложения (API) для автоматизированной загрузки сторонних списков Интернет-ссылок (URL), с учётом категорий и последующей фильтрацией
- Встроенная система автоматической классификации сайтов по содержанию страниц, распознающая не менее 100 тематических категорий (без использования облачных вычислений)
- Встроенная система предотвращения кражи данных, блокирующая передачу неизвестного шифрования, файлов с паролями и прочих транзакций, имеющих признаки шпионских
- Фильтрация сетевых коммуникационных приложений:
Система должна поддерживать: не менее 35 типов Интернет-пейджеров, не менее 30 типов одноранговых сетей P2P, не менее 25 типов систем потокового видео, не менее 25 типов приложений удалённого доступа, предотвращение обхода прокси-серверов и т.п.
- Встроенный модуль для контроля и предотвращения утечки КИ через интернет
- Встроенная система учёта вероятных инцидентов безопасности, прикрепляющая теневую копию транзакций к инцидентам, имеющим признаки нарушений политик ИБ
- Применение политик фильтрации к объектам службы каталогов (пользователи, группы, подразделения), в т.ч. с условной блокировкой трафика по времени суток, квотированием по времени и ограничением потребления трафика
- Инструмент для быстрой проверки действия фильтра по пользователю и заданному Интернет ресурсу.
- Делегирование функций управления политиками и отчётности, позволяющее изолировать применение политик безопасности и массивы сгенерированной отчётности между подразделениями организации, сохраняя при этом полную интерактивность при работе с многомерными схемами данных в рамках единого сервера управления
- Автоматическое обновление сертификатов публичных корневых центров сертификации, используемых прокси сервером для проверки

сертификатов, посещаемых сотрудниками компании веб сайтов.

- Поддержка интеграции Решения с Active Directory (обязательно через TLS/SSL).

- Веб шлюз должен иметь возможность контролировать доступ сотрудников к веб сайтам, организованный через терминальный сервер, контенту, получаемому из глобальной сети Интернет на основе категорий, приложений, распространенных протоколов, типам передаваемых файлов, времени доступа, членства в группе AD.

- Подсистема должна иметь возможность категорирования неизвестных сайтов по фактическому содержанию.

Контент-мониторинг исходящего трафика.

- Возможность выполнения контент-мониторинга как с использованием веб шлюза так и в режиме работы Агента.

- Наличие встроенной системы OCR для предотвращения утечки КИ в передаваемых графических файлах.

- Возможность настройки делегированного управления для разбора инцидентов контент-мониторинга.

- Регистрация конфиденциальных документов, хранимых в виде файлов.

- Регистрация структурированных конфиденциальных данных, хранимых в таблицах реляционных СУБД.

- Работать с различными классификаторами, такими как машинное обучение, скрипты, цифровые отпечатки, регулярные выражения, словари, ключевые слова, свойства и типы файлов. Возможность работы Endpoint агента и Веб шлюзов, для всех классификаторов должна поддерживаться как в режиме мониторинга, так и в режиме блокировки, для Endpoint агента должно поддерживаться нативное шифрование чувствительного контента, передаваемого на съёмные носители.

- Обработка всех транзакций компонентами контент-мониторинга должна осуществляться локально, без передачи транзакций на центральный сервер (в том числе при отсутствии подключения к корпоративной сети), сервера сторонних решений.

- Компоненты контент-мониторинга должны иметь возможность передачи теневой копии файла или данных для которых происходит срабатывание по политикам контент-мониторинга.

- Политики контент-мониторинга должны быть едиными для всех компонентов, либо Лицензиатом должна быть реализована автоматизация процесса создания политик для каждого компонента контент-мониторинга, таким образом, чтобы любые объекты политик (правила, классификаторы, действия) необходимо было описывать один раз.

- В рамках подсистемы контент-мониторинга должен быть модуль аналитики, осуществляющий корреляцию событий, относящихся к одному инциденту, для минимизации времени, затрачиваемых администратором на

расследование инцидента.

Компоненты подсистемы контент-мониторинга в части исходящего трафика, устанавливаемые на АРМ (называемые совместно – Агент для АРМ или Агент), должны обеспечивать возможность:

- Автономность - Агент должен быть способен защищать КИ при отключении от корпоративной сети и должен быть способен анализировать передаваемые данные в реальном режиме времени без необходимости обращения к дополнительным серверам для анализа.

- Мониторинг и блокировку исходящего трафика в случае обнаружения несанкционированной отправки КИ.

- Обнаружения конфиденциальных данных, в том числе таких как КИ и персональные данные.

- Обнаружения КИ за счет предварительного механизма обучения по примерам конфиденциальных документов. При этом Агент должен обеспечивать обнаружение КИ при использовании черновиков, модифицированных документов или их частей.

- Распознавания неконфиденциальных бланков и форм от конфиденциальных документов, построенных на базе данных бланков и форм, различение конфиденциальных и неконфиденциальных документов построенных на базе одних и тех же бланков.

- Обнаружение с возможностью последующей блокировки передачи файлов неизвестного/нестандартного формата.

- Блокирования передачи зашифрованных файлов, в том числе с использованием неизвестных заранее форматов.

- Обнаружения КИ за счет предварительного механизма обучения по примерам КИ, находящихся в СУБД. При этом Агент должен обеспечивать обнаружение КИ при использовании комбинации из небольшого числа записей и полей таблицы, а не только при работе с полными выгрузками данных.

- Разграничения доступа к КИ по приложениям. Например, агент должен обладать опцией предоставления доступа к файлу с использованием офисного пакета программ, но запрещать доступ при попытке использования SCP клиента, архиватора, шифратора и т.п.

- Безопасного обмена КИ при использовании съемных носителей. Если согласно бизнес процессам есть необходимость использования съемных носителей для обмена КИ – необходимо, не блокируя бизнес-активность, минимизировать риски утечки конфиденциальных данных. Примером подобных ситуаций может быть необходимость обмена данными между сотрудниками, находящимися вне офиса компании. При этом подсистема должна обеспечивать журналирование действий для возможности проведения служебных проверок

- Функционирование при использовании инфраструктуры VDI.

- Анализа HTTP/HTTPS трафика с АРМ. При этом, агент не должен влиять на работу системного ПО, не используемого для передачи данных.

- Анализ печати с АРМ на принтеры, как сетевые, так и физически подключенные к АРМ. При этом Система, в случае возникновения инцидента, должна предоставлять возможность администратору ИБ проанализировать исходный файл, отправленный на печать.

- Анализ копирования файлов на сетевые папки. При этом, должна поддерживаться возможность указания файловых серверов куда копирование КИ разрешено.

- Анализировать медленные утечки данных, когда утечка данных производится несколькими транзакциями. Система должна позволять указывать порог, начиная с которого можно применить блокировку транзакций.

- Получения данных из Active Directory по источнику инцидента.

- Анализа КИ, статично хранящихся на АРМ.

- Гибкого расширения за счет добавления сетевых модулей.

- Единых политик контент-мониторинга.

- Реализации оповещения владельцев данных.

- Делегирования управления на базе принципа ролевого доступа, при этом его механизмы должны предоставлять возможность разграничения доступа к инцидентам исходя из учетных записей, групп и организационных подразделений Active Directory. Например, одному из администраторов ИБ может быть разрешено анализировать инциденты пользователей входящих в определенную группу Active Directory.

- Явного назначения инцидента определенному администратору ИБ.

- Добавления тегов и комментариев к инциденту.

- Указания уровня критичности инцидента. система контент-мониторинга должна предоставлять возможность задавать собственные уровни критичности.

- Анализа сработавших правил по данному инциденту.

- Быстрого анализа части транзакции по которым сработали правила.

Интеграция:

- Решение должно иметь возможность интеграции с SIEM.

- Интеграция с Active Directory для аутентификации администраторов консоли управления или пользователей портала самообслуживания.

- Наличие управления Веб шлюзом.

Обработка TLS трафика.

- Возможность задать собственные сертификаты для использования в TLS коммуникациях.

- Для проходящих HTTPS сессий на прокси шлюзе должен поддерживаться механизм инспекции HTTPS трафика.

- Для прокси шлюза должна обеспечиваться возможность подачи инспектируемого HTTPS трафика на отдельный сетевой порт

- Для прокси шлюза должно поддерживаться автоматическое

обновление сертификатов публичных корневых центров сертификации, используемых прокси сервером для проверки сертификатов, посещаемых сотрудниками компании веб сайтов.

Работа с БД журналов

- Хранение журналов в базе данных SQL.
- Возможность создания произвольных отчетов за счет использования SQL.
- Предоставление примеров запросов для получения данных журналов.
- Поддержка доступа к СУБД с использованием TLS
- Аутентификация доступа к СУБД с использованием доменной учетной записи Active Directory.
- Возможность задания срока жизни данных в журналах. Автоматическое удаление старых данных

Функциональная подсистема повышения и проверки уровня осведомленности сотрудников должна соответствовать следующим требованиям:

- Централизованное размещение всех компонентов и элементов управления;
- Реализации веб-интерфейса для работы пользователей и администраторов;
- Поддержка функционирования в средах виртуализации VDI\$
- Обеспечение возможности работы в перспективе не менее 500 сотрудников;
- Интеграция с Active Directory для поддержания актуального списка пользователей, их ролей и расположения в структуре организации;
- Получение данных от сервера Active Directory, а также запуск принудительной синхронизации в случае необходимости;
- Возможность использования встроенного портала обучения;
- Возможность использования внешнего портала обучения (при наличии у Сублицензиата);
- Поддержка двустороннего обмена подсистемы повышения и проверки уровня осведомленности сотрудников и портала обучения, позволяющего как направлять приглашения пользователям на обучающие курсы, так и получать статистические данные об их прохождении;
- Получение подсистемой данных о событиях из различных источников данных Сублицензиата для определения необходимости назначения того или иного курса пользователю;
- Возможность тестирования связи подсистемы с источником данных, как в процессе создания подключения, так и в любое время после.

Подсистема должна включать курсы по направлениям:

1. Основы информационной безопасности

2. Защитник конфиденциальной информации
3. «Вакцинация» против фишинговых заражений
4. Рекомендации по комплексной безопасности
5. Законодательная база РФ по информационной безопасности
6. Парольная защита
7. Защита мобильных устройств

Подсистема в части повышения и проверки уровня осведомленности сотрудников должна формировать следующие виды отчетов:

- Отчет по задаче (пользователю);
- Отчет по группе задач (пользователей);
- Отчет по обучению.

Отчет по задаче (пользователю) или группе задач (пользователей) должен отражать результаты всех рассылок, проводимых с использованием заданного режима рассылки в указанную дату или период. Отчеты должны представлять собой таблицы с информацией о сотрудниках, шаблонах писем, времени прочтения писем, действиях пользователя с письмами. Результаты вывода должны фильтроваться, средствами веб-интерфейса подсистемы, включать возможность сортировки списков. Отчеты должны отражать точную текущую статистику и содержать диаграммы.

Подсистема должна:

- автоматизировать процессы выявления низкой осведомленности сотрудников Сублицензиата (пользователей АСЗИ Сублицензиата) в вопросах ИБ;
- фиксировать необходимость проведения мероприятий по повышению осведомленности сотрудников Сублицензиата в области ИБ;
- назначать им соответствующие курсы;
- обеспечивать контроль успешности прохождения курсов.

Общая схема работы подсистемы должна быть следующей:

- на основе поступающих данных о событиях ИБ и инцидентах ИБ от имеющихся у Сублицензиата информационных систем (мониторинга входящего и исходящего информационных потоков) в подсистему передается информация о деятельности пользователей;
- согласно утвержденным в подсистеме правилам выявления потребности в повышении осведомленности сотрудников Сублицензиата в области ИБ производится их направление сотрудников на необходимый курс;
- изучив краткий on-line курс, сотрудник Сублицензиата проходит тестирование для контроля успешности прохождения курса;
- подсистема должна иметь возможность использования сторонних обучающих материалов, подготовленных в формате SCORM 1.2;
- на всех этапах процесса подсистема должна предоставлять

необходимые отчеты.
Подраздел 3.3. Требования к гарантийным обязательствам оказываемых услуг
<p>Гарантийный срок внедряемой Системы должен составлять 36 месяцев с даты подписания Сторонами Акта приема-передачи прав. Гарантия не распространяется на случаи, когда отказы или снижение функциональности и/или их компонентов, отдельных функций и/или иных параметров разработанных программ произведенных настроек ПО были вызваны:</p> <ul style="list-style-type: none"> • неисправностью используемого оборудования или операционной системы; • изменениями в бизнес-процессах Сублицензиата.
Подраздел 3.4. Требования к конфиденциальности
<p>Сублицензиат и Лицензиат обязуются не использовать конфиденциальную информацию, раскрытую другой стороной, иначе как согласно Техническому заданию. Получающая сторона обязуется не копировать, не разглашать и не использовать иным способом конфиденциальную информацию без предварительного письменного одобрения другой стороной.</p>
Подраздел 3.5. Требования к безопасности оказания услуг и безопасности результата оказанных услуг
<p>Работа с документами Сублицензиата осуществляется только на площадке Сублицензиата.</p> <p>Доработка (настройка) применяемых компонентов Системы должна вестись только в защищенной среде, для целей тестирования функционала должны использовать обезличенные данные Сублицензиата.</p>
Подраздел 3.6. Требования по обучению персонала Сублицензиата
<p>Технический инструктаж 3-х специалистов Сублицензиата по эксплуатации и обслуживанию Системы.</p>
Подраздел 3.7. Требования к составу технического предложения участника
<p>Лицензиат должен предоставить действующие документы, подтверждающие право Лицензиата на распространение и обслуживание ПО на территории РФ в объеме, необходимом для Сублицензиата.</p>
Подраздел 3.8. Специальные требования
<p>Факт оказания услуг оформляется в течении 1 рабочего дня с момента окончания выполнения услуг на площадке.</p>

РАЗДЕЛ 4. РЕЗУЛЬТАТ ОКАЗАННЫХ УСЛУГ

Подраздел 4.1. Описание конечного результата оказанных услуг
Результатом оказания услуг являются предоставленное Сублицензиату право использования ПО и Система в полном составе и удовлетворяющие требованиям настоящего Технического задания.
Подраздел 4.2. Требования по приемке услуг
<p>Услуги принимаются на основании настоящего технического задания.</p> <p>Лицензиат предоставляет Сублицензиату не позднее 1 (одного) рабочего дня после окончания оказания услуг:</p> <ul style="list-style-type: none"> - Акт сдачи-приемки оказанных услуг; - Счет; - Счет-фактуру.
Подраздел 4.3. Требования по передаче Сублицензиату технических и иных документов (оформление результатов оказанных услуг)
<p>Не позднее 3 (трех) рабочих дней с момента (даты) заключения сублицензионного договора Лицензиат обязан предоставить Сублицензиату права использования ПО и направить в адрес Сублицензиата подписанный со своей Стороны Акт приема-передачи прав.</p> <p>Факт предоставления права использования ПО подтверждается подписанием обеими Сторонами Акта приема-передачи прав.</p> <p>В случае предоставления Сублицензиатом мотивированного отказа от подписания Актов Лицензиат обязан устранить выявленные Сублицензиатом замечания, в том числе привести документацию в соответствие с требованиями Договора.</p>

РАЗДЕЛ 5. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБУЧЕНИЮ ПЕРСОНАЛА СУБЛИЦЕНЗИАТА

Инструктаж по работе с Системой должен быть проведен для персонала подразделения по информационной безопасности на площадке Сублицензиата. Инструктаж должен включать как технические особенности настройки, использования Системы, так и логику работы Системы.

РАЗДЕЛ 6. ПЕРЕЧЕНЬ АББРЕВИАТУР И ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место
АСЗИ – автоматизированная система в защищенном исполнении
ИБ – Информационная безопасность

Лицензиат - Организация, выбранная для реализации проекта на основе запроса коммерческих предложений
Сублицензиат – Акционерное общество «НоваВинд»
ПО – Программное обеспечение
Система - Информационно-аналитическая система контент-мониторинга информационных потоков и действий сотрудников Сублицензиата в части информации, относящейся к конфиденциальной, включая контроль уровня и повышение осведомленности сотрудников в области информационной безопасности.
AD (Active Directory) - Служебная программа, разработанные для операционной системы Microsoft Server. Первоначально создавалась в качестве облегченного алгоритма доступа к каталогам пользователей.
DLP (Data Leak Prevention) - предотвращения утечек конфиденциальной информации.
SCORM - Sharable Content Object Reference Model, «образцовая модель объекта содержимого для совместного использования»)
SIEM - (Security information and event management) - анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений

РАЗДЕЛ 7. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ

Приложения отсутствуют

Эксперт группы информационной
безопасности и режима
АО «НоваВинд»

Д.А. Артамонов

Согласовано:
Начальник управления организации
Комплексной безопасности
АО «НоваВинд»

С.А. Овчинников

Эксперт отдела организации
закупочных процедур
АО «НоваВинд»

Н.А. Язынина