**ЧАСТЬ VI ТЕХНИЧЕСКАЯ ЧАСТЬ ДОКУМЕНТАЦИИ**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на** **поставку** **комплекса информационной безопасности для защиты периметра сети и выполнение работ по настройке и пусконаладке комплекса.**

1. **Заказчик:**  Общество с ограниченной ответственностью «ФРИИ ИНВЕСТ».
2. **Адрес Заказчика:** Российская Федерация, 101000, г. Москва, ул. Мясницкая, д. 13 стр. 18.
3. **Место выполнения работ, поставки оборудования:** Российская Федерация, 101000, г. Москва, ул. Мясницкая, д. 13 стр. 18.
4. **Предмет закупки:** поставка комплекса информационной безопасности для защиты периметра сети (далее-Комплекс) и выполнение работ по настройке и пусконаладке
5. Поставка Комплекса и выполнение работ (далее - Работы) осуществляются по адресу: г. Москва, ул. Мясницкая, д. 13, стр. 18 (далее – «Объект») в соответствии с требованиями настоящего Технического задания.
6. **Срок поставки Оборудования и выполнения Работ:** Исполнение обязательств по Договору осуществляется в два этапа:

Первый этап - поставка Комплекса.

Срок поставки: не позднее 23 декабря 2022г.Частичная поставка не допускается*.*

Второй этап: выполнение Работ. Все Работы выполняются в течение 15 рабочих дней с даты поставки Комплекса и подписания Акта приема-передачи.

1. **Порядок оплаты:** Оплата по соответствующему этапу договора осуществляется в течение 14 (Четырнадцати) рабочих дней с даты подписания Акта приема-передачи Комплекса/Акта выполненных работ по каждому этапу договора путём перечисления денежных средств на расчётный счёт Поставщика при условии выставления счета Поставщиком. Авансирование не предусмотрено.
2. **Цели выполнения работ, поставки оборудования:**
	1. Комплекс информационной безопасности предназначен для обеспечения безопасности корпоративной информационной вычислительной сети Заказчика от внешних интернет-угроз, обеспечения управление трафиком и шириной канала, контроля политики доступа в сеть Интернет и использования интернет-приложений, а также для безопасного удаленного доступа сотрудников к внутренним сетевым ресурсам.
	2. Комплекс информационной безопасности должен заменить используемое оборудование Cisco на аналогичное российское решение.
3. **Требования к составу Комплекса и выполнению работ:**
	1. **Состав Комплекса**

|  |  |  |
| --- | --- | --- |
| **№** | **Описание** | **Количество** |
| 1 | Межсетевой экран (МСЭ) | 2 |
| 2 | Система централизованного сбора, анализа и регистрации логов и событий, построения отчетов | 1 |

* 1. **Технические требования к оборудованию и программному обеспечению**

#####

Поставляемое оборудование должно быть собрано в промышленных условиях, удовлетворяющих стандарту ISO9001, иметь сертификаты соответствия требованиям системы сертификации ЕАС.

Должны быть установлены и настроены все обновления, доступные на момент приобретения оборудования, все драйвера чипсета и устройств, входящих в комплектацию оборудования, а также необходимые утилиты, обеспечивающие полноценное функционирование МСЭ;

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование товара** | **Характеристика товара** | **Значение характеристики**  |
| **1.** | **Межсетевой экран** | **Технические требования** |
| На передней панели корпуса:USB 2.0 Ports  | 2 шт. (значение не меняется). |
| Типоразмер корпуса | 1 U (значение не меняется) |
| Габариты (ШхВхГ) | 438x44x580 мм(значение не меняется) |
| Цвет корпуса | Однотонный (значение не меняется) |
| Материал корпуса | Сталь (значение не меняется) |
| Вентиляторы на задней стенке корпуса  | 4 шт. (значение не меняется) |
| Количество слотов памяти  | 4 шт. (значение не меняется) |
| Количество разъемов PCI-E 4x | 1 (значение не меняется) |
| Сетевой контроллер | 10/100/1000 Мегабит (значение не меняется) |
| Дополнительные слоты для установки 10 гигабит адаптеров | 2 (значение не меняется) |
| Внешние порты ввода-вывода (все указанные порты должны быть свободными)COMRJ45D-subUSB 2.0 | 1 шт. (значение не меняется)8 шт. (значение не меняется)1 шт. (значение не меняется)2 шт. (значение не меняется) |
| Объем памяти  | 32 Гб (значение не меняется) |
| Тактовая частота | 1600 МГц (значение не меняется) |
| **Процессор:** |  |
| Количество ядер  | 8 (значение не меняется) |
| Базовая частота процессора  | 1800 МГц (значение не меняется) |
| Количество вычислительных потоков | 16 шт. (значение не меняется) |
| Максимальная тактовая частота с технологией Turbo Boost | 2300 МГц (значение не меняется) |
| Типичное тепловыделение | 70 Вт (значение не меняется) |
| **Блок питания:** | 2 шт. (значение не меняется) |
| Мощность | 300W (значение не меняется) |
| **НЖМД :** |  |
| Форм-фактор  | 2.5 дюйма (значение не меняется) |
| Объем  | 1000 Гб (значение не меняется) |
| Интерфейс SATA | 6Gb/s (значение не меняется) |
| Скорость вращения шпинделя | 7200 об/мин. (значение не меняется) |
| Буфер НЖМД | 128 Мб (значение не меняется) |
| Время продолжительности беспрерывной работы  | 1.4 млн. часов (значение не меняется) |
| Количество НЖМД | 2 шт. (значение не меняется) |
|  |  | Управление по IMPI | Наличие |
|  |  | Год выпуска  | Не ранее 2020 |
|  |  | **1. Функциональные требования*** 1. Контроль доступа пользователей в сеть Интернет и фильтрации трафика сети Интернет с обеспечением защиты от вредоносного программного обеспечения;
	2. Анализ трафика сети Интернет по категориям сайтов, URL-адресам и контенту данных;
	3. Мониторинг действий, совершаемых пользователями при работе с сетью Интернет, а также формирование отчетности;
	4. Предоставление возможности объединения офисов компании в общую сеть посредством VPN-соединений с помощью протокола L2TP/IPSec;
	5. Предоставление доступа к внутренним ресурсам компании мобильным сотрудникам компании посредством VPN L2TP/IPsec с аутентификацией посредством Radius/Active Directory c использованием операционных систем Microsoft Windows, MacOS. Android, iOS ;
	6. Предоставление или ограничение доступа к внутренним сетевым ресурсам на основании принадлежности к доменным группам при подключении пользователей по VPN;
	7. Обеспечение отказоустойчивости и высокой доступности подключений VPN;
	8. Предоставление возможности обновлять списки с помощью офлайн обновлений;
	9. Защита объектов сетевой инфраструктуры заказчика от DoS атак;
	10. Возможность встраивания в сетевую инфраструктуру заказчика по протоколу WCCP;
	11. Защита объектов сетевой инфраструктуры с помощью системы обнаружения вторжений (СОВ);
	12. Контроль передаваемого трафика через МСЭ с помощью определения приложений L7.
	13. Инспектирование и контроль передаваемого SSH и SSL трафика
	14. Поддержка агрегирования физических каналов (LACP), совместимость с коммутаторами Extreme x460;
	15. Поддержка подинтерфейсов, возможность маршрутизации между подинтерфейсами, создание списков доступа между подинтерфейсами;
	16. Поддержка VLAN (802.1Q);
	17. Поддержка DHCP на подинтерфейсах;
	18. Возможность автоматического переключения на резервный канал в Интернет при отказе основного канала.
1. **Особенности реализации функций**
	1. Функционал настройки средств фильтрации входящего и исходящего трафика должен позволять указывать в качестве фильтра маску или регулярное выражение.
	2. Должна быть обеспечена возможность применения правил МСЭ к фрагментированным, нефрагментированным и любым другим пакетам.
	3. Необходимо наличие события об успешной загрузке системы в журнале событий.
	4. Должно быть обеспечено журналирование изменения времени в консоли администрирования.
	5. Необходимо наличие оповещений по SNMP при срабатывании запрещающих правил межсетевого экрана.
	6. Должна обеспечиваться блокировка всего трафика при инцидентах, таких как нарушение функционирования системы. В случае если исполняемый файл из состава МСЭ изменен, весь трафик должен быть заблокирован.
	7. Функционал решения должен иметь возможность запрашивать ввод пароля на разблокировку в случае несанкционированного доступа к изменениям правил МСЭ, изменениям правил оповещения, сетевым интерфейсам, добавлению учетной записи нового администратора, экспорту логов системы.
	8. Должна быть обеспечена возможность удаленного подключения технической поддержки в случае полного падения системы (решения).
	9. Фильтрация входящего и исходящего Интернет-трафика должна осуществляться с одновременным обеспечением проверки на наличие вредоносного программного обеспечения.
	10. Средства, реализующие функционал мониторинга работоспособности и формирования отчетности, должны предоставлять функционал автоматизированного получения данных о действиях пользователей, совершаемых в сети Интернет, от средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.
	11. Средства контроля доступа в сеть Интернет и фильтрации трафика сети Интернет, должны предоставлять следующую функциональность:
* работать в качестве непрозрачного и прозрачного сервера-Интернет и обеспечивать кэширование HTTP;
* поддерживать аутентификацию пользователей, интегрироваться с доменами, построенными на базе Microsoft Active Directory и поддерживать технологию Single Sign-On;
* поддерживать аутентификацию пользователей с внешними серверами Radius, Kerberos, NTLM, Active Directory, локальной базой учетных записей;
* поддерживать идентификацию пользователей с помощью протокола Radius accounting;
* поддерживать идентификацию локальных пользователей по IP/MAC-адресам, идентификаторам VLAN;
* поддерживать аутентификацию пользователей, работающих на терминальных серверах Microsoft Windows, и на рабочих станциях, работающих под управлением ОС Microsoft Windows, с использованием агентов авторизации.
* обеспечивать разделение прав при доступе к сети Интернет на основе доменных и локальных групп и поддерживать управление разрешениями;
* обеспечивать фильтрацию передаваемого контента и блокировку определенных типов файлов, в том числе в SSL-трафике, включая трафик, зашифрованный с помощью протокола TLSv1.3 и SSL-трафик, зашифрованный с помощью криптоалгоритмов ГОСТ.
* обеспечивать фильтрацию передаваемого SSH-трафика с возможностью блокировки определенных команд SSH;
* предоставлять функционал гибкой настройки правил фильтрации на основе различных параметров, в частности, групп доступа пользователей и типов передаваемого контента;
* предоставлять интегрированные механизмы оповещения и уведомления администраторов и пользователей о событиях;
* предоставлять клиента для авторизации на АРМ пользователей;
* предоставлять возможность применения фильтрации на основе информации о реферере;
* предоставлять возможность применения правил в указанные временные интервалы.
1. **Требования к доступности и производительности**
	1. Программное обеспечение должно иметь возможность быть реализованным в соответствии с методом обеспечения высокой доступности, гарантируя минимальное время простоя, и полного решения возложенных задач при выходе из строя одного из компонентов.
	2. Программное обеспечение должно обеспечивать резервное копирование конфигураций компонентов и журналов регистрации событий с функцией исторического хранения данных с глубиной хранения не менее 12 месяцев.
	3. Программное обеспечение должно обеспечивать доступ в сеть Интернет не менее чем для 1000 пользователей, подключенных к Интернет, при этом не оказывая влияния на скоростные показатели доступа пользователей в сеть Интернет и не препятствуя функционированию компонентов корпоративной информационной вычислительной сети Заказчика.
	4. Пропускная способность МСЭ, трафик EMIX: не менее 20 Гб/с;
	5. Одновременное количество TCP сессий: не менее 10Млн;
	6. Количество новых соединений: не менее 50000 в сек;
	7. Пропускная способность СОВ, трафик EMIX:

 не менее 2 Гб/с;* 1. Инспектирование SSL, трафик EMIX: не менее 3 Гб/c
	2. Производительность МСЭ на уровне контроля приложений c функцией определения приложений L7, СОВ, контентная фильтрация, трафик EMIX: не менее 2.5 Гб/с;
	3. Программное обеспечение должно иметь возможность масштабирования. Увеличение числа обслуживаемых пользователей и объема обрабатываемого трафика сети Интернет должно осуществляться путем подключения дополнительных программно-аппаратных компонентов.
	4. При наличии дополнительных узлов программное обеспечение должно позволять в любое время выводить часть узлов фильтрации из эксплуатации для обслуживания с автоматическим перераспределением нагрузки на оставшиеся узлы прозрачно для пользователей.
	5. Должен обеспечиваться функционал настройки программно-аппаратных средств, входящих в состав, без прерывания работоспособности МСЭ.
	6. Программное обеспечение должно обеспечивать функцию планового отключения для выполнения профилактических мероприятий, изменений или наращивания аппаратного обеспечения, установки обновлений на программное обеспечение.
	7. Программное обеспечение должно предоставлять инструменты диагностирования состояния собственных компонентов.
	8. В Программном обеспечении должна быть предусмотрена ролевая модель разграничения доступа. Роли должны иметь ограничения по доступу к Программному обеспечению на уровне интерфейсов, функционала, отчетов и производственных объектов.
1. **Требования к функционалу средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.**
	1. Обеспечение и контроль доступа пользователей в сеть Интернет с фильтрацией входящего и исходящего Интернет-трафика по протоколам HTTP/HTTPS.
	2. Проверка подлинности пользователей при доступе в сеть Интернет с использованием службы каталогов Microsoft Active Directory.
	3. Контроль доступа пользователей в сеть Интернет с функционалом установки различных политик доступа для различных групп пользователей на основе членства в группах безопасности службы каталогов Microsoft Active Directory.
	4. Управление доступом в сеть Интернет программ и сетевых служб путём разрешения и назначения портов.
	5. Отключение функционала контроля доступа в сеть Интернет и фильтрации трафика сети Интернет для конкретных пользователей/IP-адресов.
	6. Управление доступом пользователей к различным типам информации в сети Интернет (видео, аудио, изображения и т.д.).
	7. Предоставление интерфейса гибкой настройки правил фильтрации на основе различных параметров, в частности, групп доступа пользователей, категорий ресурсов (в том числе и ресурсов, не отнесенных ни к одной из категорий) и типов передаваемого контента.
	8. Настраиваемые оповещения администраторов МСЭ о событиях в работе средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.
	9. Уведомление в окне браузера пользователя сети Интернет о блокировании доступа к запрашиваемому пользователем web-ресурсу в случае нарушения корпоративных требований информационной безопасности, а также на основании наличия потенциально опасного кода (с функцией правки кода и текста уведомления).
2. **Требования к функционалу средств мониторинга и отчетности МСЭ**
	1. Протоколирование действий пользователей и администраторов МСЭ.
	2. Возможность, в режиме on-line, отслеживания текущей сессии пользователя, определения сервера, через который установлена сессия, подключения к серверу и разбора пользовательской сессии.
	3. Определение геолокации на основе IP-адреса домена.
	4. Формирование отчетности с функционалом:
* объявления пользовательских (новых) полей
* формирования запросов с использованием перекрестных запросов.
	1. Формирование отчетности с предоставлением функционала:
* задания фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности;
* формирования запросов к базе данных;
* задания формата отчетов.
	1. Отправку отчетов по расписанию и по запросу администраторов МСЭ.
	2. Отключение мониторинга функционирования и формирования отчетности для конкретных пользователей/IP-адресов.
	3. Автоматическое или ручное обновление компонентов с сайта производителя.
	4. Управление доступом к средствам мониторинга и отчетности с использованием ролевой модели.
	5. Отправка статистической информации по протоколу NetFlow версий 5, 9, 10.
1. **Связь с существующим окружением и интеграция**
	1. Разграничение полномочий доступа для работы с МСЭ и доступа пользователей в сеть Интернет должно быть реализовано на ролевой основе с использованием групп существующих доменов Active Directory.
	2. МСЭ должен взаимодействовать со следующими смежными системами:
* Система Active Directory, в части аутентификация пользователей в Active Directory, определение принадлежности пользователей к группам Active Directory.
* Системами авторизации пользователей Kerberos, NTLM, Single-Sign-On в части автоматической авторизации пользователей.
* Система идентификации пользователей Radius accounting, определение IP-адресов пользователей.
* Система синхронизации времени, в части взаимодействия с системой синхронизации времени должна поддерживать определение точного времени.
* Система доменных имен (DNS), в части взаимодействия с системой DNS должно поддерживать определение IP-адресов узлов сети по имени узла.
* Система мониторинга SNMP, в части взаимодействия с системой мониторинга SNMP должно поддерживать оповещение и работу в режиме запросов состояния системы по протоколам SNMP v2 и SNMP v3.
* Корпоративная почтовая система (E-mail), в части взаимодействия с корпоративной почтовой системой должно поддерживать отправку по e-mail оповещений администраторам о событиях в работе средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.
* Система сбора и корреляции событий информационной безопасности, в части взаимодействия с системами сбора и корреляции событий информационной безопасности должно предоставлять механизм экспорта журнальных сообщений в режиме реального времени. Формат и детализация данных сообщений должны настраиваться.
* Системы дополнительного контентного анализа, в части взаимодействия с системами дополнительного контентного анализа должно предоставлять модуль интеграции по протоколу I-CAP с указанными системами в части условий доступа на основании результатов анализа контента.
1. **Требования к пользовательскому интерфейсу**
	1. Программный интерфейс компонентов МСЭ, включая средства управления, а также формы оповещений и уведомлений администраторов МСЭ и пользователей сети Интернет должен полностью поддерживать русский язык, используя кодировку текста UTF-8.
	2. Наличие web-интерфейса для доступа к компонентам узла фильтрации Интернет-трафика, включая средства управления, полностью поддерживающего русский язык, используя кодировку текста UTF-8.
2. **Требования к наличию отчетов**
	1. МСЭ должен обеспечивать формирование отчетности в табличном и графическом виде о совершаемых пользователями действиях в сети Интернет за различные периоды времени
3. **Требования к системе обнаружения вторжений в составе МСЭ**
	1. Система должна обеспечивать защиту от известных атак на основе сигнатурного анализа трафика.
	2. Система должна иметь возможность работы в режиме детектирования атак, так и в режиме предотвращения атак.
	3. Система должна иметь возможность применять различные профили сигнатур к различному типу трафика.
	4. Система должна позволять создавать исключения из проверки для определенного типа трафика.
	5. Система должна обеспечить запись событий (журналирование) сработанных правил в соответствующий журнал.
4. **Требования к системе определения приложений L7 в составе МСЭ.**
	1. Система должна обеспечивать определение трафика приложений на основе сигнатурного анализа трафика.
	2. Система должна иметь возможность блокировать определенные группы сигнатур приложений для различного типа трафика.
	3. Система должна обеспечить запись событий (журналирование) сработанных правил в соответствующий журнал.
5. **Требования к системе инспектирования трафика SSH в составе МСЭ.**
	1. Система должна обеспечивать дешифрование SSH-трафика.
	2. Система должна иметь возможность блокировать определенные команды, передаваемые внутри протокола SSH.
	3. Система должна иметь возможность блокировать передачу файлов, передаваемых с помощью протокола SFTP.
6. **Дополнительные требования**
	1. Автоматическое или ручное обновление программных компонентов с сайта производителя.
	2. Управление доступом к средствам контроля доступа в сеть Интернет и фильтрации трафика сети Интернет с использованием ролевой модели.
	3. Протоколирование действий администраторов МСЭ.
	4. Предоставление возможности автоматического развертывания серверов фильтрации трафика с использованием API.
 |
| **2** | **Система централизован-ного сбора, анализа и регистрации логов и событий, построения отчетов** | **Функциональные требования**Система сбора логов, журналов с межсетевых экранов должна поставляться в виде виртуального образа для VMware для организации выделенного сервера мониторинга функционирования, формирования отчетности. Должна быть совместима с поставляемыми МСЭ.Программное обеспечение должно обладать следующей функциональностью:Система мониторинга функционирования и формирования отчетности должна позволять осуществлять мониторинг работы систем МСЭ в режиме реального времени при помощи журналов событий, веб-доступа, СОВ и трафика.У администратора должна быть возможность настроить автоматический экспорт журналов на сервера по протоколам SSH, FTP и Syslog.Отчеты должны предоставлять различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей.Формирование отчетов по созданным ранее правилам и шаблонам в автоматическом режиме и отправка адресатам по электронной почте.Протоколирование действий пользователей и администраторов нескольких систем МСЭ.Формирование отчетности с предоставлением функционала:Задания фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности;Формирования запросов к базе данных;Задания формата отчетов.Определение геолокации на основе IP-адреса домена.Отправку отчетов по расписанию и по запросу администраторов Системы.Автоматическое или ручное обновление компонентов с сайта производителя. |

* 1. **Требования к происхождению**
		1. Входящие в состав Программного обеспечения Комплекса программные компоненты должны быть российского производства и внесены в Единый реестр российских программ для электронных вычислительных машин и баз данных.
	2. **Требования к упаковке**
		1. Поставка должна производиться в запечатанной упаковке, обеспечивающей сохранность содержимого и невозможность использования третьими лицами без ее повреждения.
1. **Состав Работ:**

Работы включают в себя полную настройку и ввод в эксплуатацию Комплекса в имеющуюся инфраструктуру заказчика, а именно:

* + 1. Обследование инфраструктуры заказчика
		2. Разработка и согласование с Заказчиком предложения по применяемым настройкам Комплекса
		3. Коммутация оборудования (производится согласно требованиям по коммутации, предоставляемым Заказчиком);
		4. Первоначальная настройка МСЭ;
		5. Подключение и настройка МСЭ, в соответствии с конфигурацией имеющихся межсетевых экранов (МСЭ) Cisco ASA, в том числе:
			1. Настройка агрегирования 6 физических интерфейсов;
			2. Настройка подинтерфейсов в соответствии конфигурацией, имеющихся МСЭ;
			3. Перенос существующих правил NAT и ACL;
			4. Настройка интеграции МСЭ Комплекса с MS Active Directory;
			5. Настройка удаленного подключения пользователей по протоколу L2TP IPSec с аутентификацией в Active Directory, существующей у Заказчика;
			6. Настройка автоматического переключения на резервного провайдера при отказе основного.
		6. Сверка функционала с настройками МСЭ Cisco в настройках
		7. Замена МСЭ Cisco, установленных на периметре сети в офисе и в ЦОД, на МСЭ Комплекса с сохранением функционирования всех сервисов;
		8. Настройка системы обнаружения вторжений;
		9. Настройка системы централизованного сбора и анализа журналов МСЭ (сервер предоставляется Заказчиком)

Всю информацию для настроек предоставляет сторона Заказчика;

1. **Требования к качеству выполнения работ:**

1) работы должны быть выполнены в полном объеме и в установленные сроки;

2) работы должны выполняться в соответствии с действующими стандартами и рекомендациями, соблюдением объектовых режимов и правил техники безопасности;

3) специалисты, привлекаемые к выполнению работ, должны иметь необходимую квалификацию и опыт для работы с поставляемым оборудованием;

4) контроль качества выполняемых работ должен осуществляться на всех этапах выполнения исполнения договора с привлечением представителей Заказчика.

**12.** **Требования к гарантийным обязательствам:**

1)гарантийный срок на оборудование составляет не менее 24 (двадцати четырех) месяцев;

2) гарантийный срок на результат выполненных работ – не менее 12 месяцев.

3) гарантийный срок исчисляется с момента подписания акта выполненных работ;

4) в составе поставляемых с товарами информационных материалов должны быть указаны условия выполнения гарантийных обязательств и номера контактных телефонов сервисных центров;

5) гарантийное обслуживание оборудования должно осуществляться Исполнителем. Доставка оборудования обеспечивается силами и за счёт средств Исполнителя;

6) гарантия должна распространяться на всё поставляемое оборудование и работы. Все расходы по гарантийному обслуживанию несет Исполнитель;

7) все запасные части, которые Исполнитель устанавливает на оборудование в течение гарантийного срока, должны быть произведены тем же производителем, что и исходные комплектующие оборудования.

**13. Требования к специалистам Исполнителя:**

1) в составе специалистов, привлекаемых к выполнению работ по настройке и пусконаладке, должны быть специалисты, обладающие сертификатами, подтверждающими их квалификацию в соответствии с настоящим Техническим заданием;

2) перечень сертификатов, которыми должны обладать сотрудники:

| **Тип оборудования** | **Сертификат** |
| --- | --- |
|  | Согласно предлагаемому типу |

Директор департамента Подосенин А.А.

информационных технологий