

УТВЕРЖДАЮ

Заместитель генерального директора –
директор по безопасности

Ю.В. Гагарин
« ____ » _____ 2022 г.

Техническое задание
на поставку групп товаров

Предмет закупки: Поставка многофункционального программно-аппаратного
решения для организации защищенного доступа в Интернет

Москва
2022

22.04.2022 341-1.7/163

Подписан простой электронной подписью
--

Техническое задание

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПЕРЕЧЕНЬ ТОВАРОВ И ОБЩИХ ТРЕБОВАНИЙ.....	3
РАЗДЕЛ 2. СВЕДЕНИЯ О НОВИЗНЕ	4
РАЗДЕЛ 3. ТРЕБОВАНИЯ К МАРКИРОВКЕ	4
РАЗДЕЛ 4. ТРЕБОВАНИЯ К УПАКОВКЕ	4
РАЗДЕЛ 5. ТРЕБОВАНИЯ ПО ПРАВИЛАМ СДАЧИ И ПРИЕМКИ	4
Подраздел 5.1 Порядок сдачи и приемки	4
Подраздел 5.2 Требования по передаче заказчику технических и иных документов при поставке товаров.....	4
РАЗДЕЛ 6. ТРЕБОВАНИЯ К ТРАНСПОРТИРОВАНИЮ	4
РАЗДЕЛ 7. ТРЕБОВАНИЯ К ХРАНЕНИЮ	4
РАЗДЕЛ 8. ТРЕБОВАНИЯ К ОБСЛУЖИВАНИЮ	5
РАЗДЕЛ 9. ЭКОЛОГИЧЕСКИЕ ТРЕБОВАНИЯ	5
РАЗДЕЛ 10. ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ	5
РАЗДЕЛ 11. ТРЕБОВАНИЯ К КАЧЕСТВУ	5
РАЗДЕЛ 12. ТЕХНИЧЕСКОЕ СОПРОВОЖДЕНИЕ ГРУПП ТОВАРОВ, ЗА ИСКЛЮЧЕНИЕМ НЕСТАНДАРТНОГО ОБОРУДОВАНИЯ.....	5
РАЗДЕЛ 13. ДОПОЛНИТЕЛЬНЫЕ (ИНЫЕ) ТРЕБОВАНИЯ.....	5
РАЗДЕЛ 14. ТРЕБОВАНИЕ К ФОРМЕ ПРЕДСТАВЛЯЕМОЙ ИНФОРМАЦИИ.....	5
РАЗДЕЛ 15. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБУЧЕНИЮ ПЕРСОНАЛА ЗАКАЗЧИКА	5
РАЗДЕЛ 16. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ	6
РАЗДЕЛ 17. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ.....	6
ПРИЛОЖЕНИЕ № 1 К ТЕХНИЧЕСКОМУ ЗАДАНИЮ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ.....	7

РАЗДЕЛ 1. ПЕРЕЧЕНЬ ТОВАРОВ И ОБЩИХ ТРЕБОВАНИЙ

1	2	3	4	5	6	7	8	9	10	11
№ п/п	Наименование	Основные технические характеристики товара	Параметры определения соответствия аналогов	Комплектность	Единица измерения	Данные из ниже при- веденного перечня	Количе- ство	Срок по- ставки	Место по- ставки	Объем гарантий и гарантийный срок
1	Программно-аппаратный комплекс «Межсетевой экран с системой обнаружения вторжений Idesco UTM» для обеспечения задачи безопасного межсетевого взаимодействия, учета и контроля использования ресурсов глобальной сети Интернет (или аналог)	Приложение №1	Приложение №1	Приложение №1	шт.	Код ОКДП 2 26.20.40.140	2 шт.	15 рабочих дней от даты подпи- сания дого- вора	Москва, Каширское шоссе, д. 3, корп. 2, стр.16, деловой квартал «Сириус Парк»	Гарантия на аппаратную компоненту – 1 год Срок технической поддержки ПО – 12 месяцев.

РАЗДЕЛ 2. СВЕДЕНИЯ О НОВИЗНЕ

Поставляемый товар должен быть новым, выпуска не ранее 2021 года, не являться выставочным образцом, не бывшим в употреблении, не восстановленным, и быть свободным от прав третьих лиц.

Технические характеристики, подтверждающие его новизну - это отметки и штампы на лицензии и в сопроводительных документах.

Исключается незаконное использование чужих товарных знаков, знаков обслуживания, фирменных наименований, патентов, полезных моделей, промышленных образцов, наименований места происхождения товара.

При использовании Поставщиком (Изготовителем) товарных знаков, знаков обслуживания, фирменных наименований, патентов, полезных моделей, промышленных образцов других правообладателей в составе сопроводительных документов на продукцию дополнительно предоставляется подтверждение правообладателя (официального дистрибьютера) о возможности использования продукции его производства с использованием данных товарных знаков, знаков обслуживания, фирменных наименований, патентов, полезных моделей, промышленных образцов, или сертификат соответствия, или декларация о соответствии с гарантией для продукции от производителя (изготовителя) такой продукции.

До осуществления поставки продукции Поставщиком (Изготовителем) осуществляется проверка на отсутствие признаков ее принадлежности к КФПСП в соответствии с пунктами 4.2 и 4.3 ЕОМУ КФПСП

[http://zakupki.rosatom.ru/?mode=CMSArticle&action=siteview&oid=1090&returnurl=&n](http://zakupki.rosatom.ru/?mode=CMSArticle&action=siteview&oid=1090&returnurl=&node=mbb)
ode=mbb;

При выявлении Поставщиком (Изготовителем) признаков КФПСП поставка такой продукции Заказчику не допускается.

РАЗДЕЛ 3. ТРЕБОВАНИЯ К МАРКИРОВКЕ

Способ нанесения маркировочных обозначений на носитель дистрибутива должен обеспечивать сохранность и четкое их прочтение в течение всего срока службы носителя.

РАЗДЕЛ 4. ТРЕБОВАНИЯ К УПАКОВКЕ

Необходимо обеспечить надежную стандартную упаковку и принять меры по его защите от воздействия влаги и прямого света.

РАЗДЕЛ 5. ТРЕБОВАНИЯ ПО ПРАВИЛАМ СДАЧИ И ПРИЕМКИ

Подраздел 5.1 Порядок сдачи и приемки

Оборудование поставляется Поставщиком непосредственно по адресу Заказчика: Заказчик: Москва, Каширское шоссе, д. 3, корп. 2, стр.16, деловой квартал «Сириус Парк». Датой поставки оборудования считается дата подписания акта сдачи-приемки обеими сторонами.

Подраздел 5.2 Требования по передаче заказчику технических и иных документов при поставке товаров

Поставщик передает Заказчику следующие документы:

- ТОРГ12 в 2 экз.
- счёт-фактура в 1 экз.
- акт сдачи-приёмки в 2 экз.
- сертификат (ФСТЭК) в 1 экз.

РАЗДЕЛ 6. ТРЕБОВАНИЯ К ТРАНСПОРТИРОВАНИЮ

Специальные требования, исходя из характера товара, не предъявляются.

РАЗДЕЛ 7. ТРЕБОВАНИЯ К ХРАНЕНИЮ

Специальные требования, исходя из характера товара, не предъявляются.

РАЗДЕЛ 8. ТРЕБОВАНИЯ К ОБСЛУЖИВАНИЮ

Специальные требования, исходя из характера товара, не предъявляются.

РАЗДЕЛ 9. ЭКОЛОГИЧЕСКИЕ ТРЕБОВАНИЯ

Специальные требования, исходя из характера товара, не предъявляются.

РАЗДЕЛ 10. ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ

Специальные требования, исходя из характера товара, не предъявляются.

РАЗДЕЛ 11. ТРЕБОВАНИЯ К КАЧЕСТВУ

Поставщик несет единоличную ответственность за качество товара перед Покупателем.

РАЗДЕЛ 12. ТЕХНИЧЕСКОЕ СОПРОВОЖДЕНИЕ ГРУПП ТОВАРОВ, ЗА ИСКЛЮЧЕНИЕМ НЕСТАНДАРТНОГО ОБОРУДОВАНИЯ

Техническая поддержка осуществляется в течение 1 года с даты поставки.

РАЗДЕЛ 13. ДОПОЛНИТЕЛЬНЫЕ (ИНЫЕ) ТРЕБОВАНИЯ

Дополнительные требования не предъявляются.

РАЗДЕЛ 14. ТРЕБОВАНИЕ К ФОРМЕ ПРЕДСТАВЛЯЕМОЙ ИНФОРМАЦИИ

Требования к форме предоставляемой информации не предъявляются.

РАЗДЕЛ 15. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБУЧЕНИЮ ПЕРСОНАЛА ЗАКАЗЧИКА

Требования к техническому обучению персонала отсутствуют.

РАЗДЕЛ 16. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

№ п/п	Сокращение	Расшифровка сокращения
1	ПО	Программное обеспечение
2	ФСТЭК	Федеральная служба по техническому и экспортному контролю
3	СНГ	Содружество независимых государств
4	МЭ	Межсетевой экран

РАЗДЕЛ 17. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ

№ п/п	Наименование приложения	Номер страницы
1	Технические характеристики	7

_____ А.В. Аленичев

ПРИЛОЖЕНИЕ № 1 К ТЕХНИЧЕСКОМУ ЗАДАНИЮ

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Программно-аппаратный комплекс «Межсетевой экран с системой обнаружения вторжений Ideco UTM» (или аналог) для обеспечения задачи безопасного межсетевого взаимодействия, учета и контроля использования ресурсов глобальной сети Интернет для 1500 пользователей

Программно-аппаратный комплекс должен включать в себя:

1. Аппаратную компоненту с характеристиками:

Тип корпуса: высота не более 87 мм., ширина – не более 438 мм., длина – не более 659 мм. Возможность для крепления в стойку, форм-фактор 2U.

Процессор: Intel Xeon Silver 4210 [10 ядер, 20 потоков, 2,2 Гц, 13,75 Мб кэш, 85 Вт] или аналог не менее 10-ти ядер (20 потоков).

Оперативная память: не менее 32GB DDR4.

Хранилище: не менее одного SSD, объемом не менее 240GB SATA.

Сетевые Ethernet интерфейсы: не менее 4 шт.

Источник питания: двоянный блок питания не менее 800 Вт (2*800 Вт).

Сервер должен быть включен в реестр промышленной продукции, произведенной на территории Российской Федерации.

2. Программную компоненту.

Программный комплекс должен соответствовать следующим требованиям по безопасности информации: «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012), «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020).

Программное обеспечение должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Программный комплекс должен базироваться на ядре Linux (версии ядра не ниже 5.11).

В системе должен присутствовать модуль постоянного слежения за системой, предотвращающий возможность нарушения работы служб при выходе параметров их работы за определенные установленные рамки.

При загрузке, системой должны быть проверены все параметры оборудования, состояние файловой системы и баз данных, а также контрольная сумма всех неизменяемых файлов.

Должна использоваться система автоматического обновления, которая позволяет своевременно переходить на новые версии ПО. Все загружаемые файлы должны проверяться электронной цифровой подписью, для обеспечения гарантии целостность и подлинность загружаемых данных.

Для доступа в Интернет для каждого пользователя должна быть предусмотрена аутентификацию по логину и паролю через VPN PPTP, IKEv2/IPSec, L2TP/IPSec, SSTP, идентификация по IP адресу, MAC адресу, аутентификация через WEB. При аутентификации через VPN должна быть обеспечена защита от прослушивания трафика и подстановки IP-адреса. Должна быть предусмотрена синхронизация пользователей через Active Directory и LDAP сервер, их прозрачная (Single Sign-On) аутентификация по протоколу Kerberos, NTLM и по логам безопасности контроллера домена. В том числе возможность интеграции с несколькими независимыми доменами Active Directory.

Вся информация о пользователях должна храниться в базе данных sqlite. Пароли пользователей и административных учетных записей не должны храниться в открытом виде. Система должна хранить детализированную статистику каждого пользователя и каждой группы. В любой момент времени должна быть предусмотрена возможность посмотреть в форме отчета, какие ресурсы Интернет посещал пользователь или вся группа. Подсчет статистической информации должен вестись в реальном времени, с автоматическим предупреждением и отключение пользователя при превышении установленных лимитов. Статистика посещения ресурсов Интернет должна вестись в Мб.

В программной компоненте должна быть предусмотрена система автоматического резервного копирования базы данных, конфигурационных файлов и, опционально, каталогов, указанных пользователем на FTP-сервер или общие папки Windows.

Система должна включать в себя возможность создания отказоустойчивого кластера в режиме Active/Passive.

В систему должна быть встроена возможность управления с локальной консоли с полным доступом к файловой системе и системным командам (в том числе удаленный доступ из доверенного контура по протоколу SSH), через WEB интерфейс. Система должна поддерживать возможность использования нескольких учетных записей администратора для администрирования через WEB интерфейс.

Программный комплекс должен функционировать как маршрутизатор, поддерживающий неограниченное число интерфейсов (как локальных, так и внешних). Поддерживать виртуальные 802.1q VLAN интерфейсы, PPTP, PPPoE интерфейсы. Возможность указать маршруты по источнику, назначению.

Система должна обеспечивать поддержку нескольких каналов провайдеров и нескольких внешних сетей. Возможность полного разделения пользователей для выхода в Интернет через разных провайдеров. Автоматическую проверку связи с провайдером и переключение на альтернативного провайдера, в случае необходимости. Подключение к провайдеру по протоколам PPTP VPN, PPPoE и L2TP. Возможность балансировки трафика между каналами.

В системе должна быть предусмотрена возможность включения функции контент-фильтра, позволяющего управлять доступом к сайтам определенных категорий (не менее 144 категорий сайтов, и не менее 500 млн. url в базе данных). Должна иметься возможность фильтрации скачиваемых файлов по расширению и MIME-типам. Также, в соответствии с категориями сайтов должна формироваться веб-отчетность по трафику пользователей. Контент-фильтр должен фильтровать как HTTP, так и HTTPS-трафик, как с его расшифровкой, так и без расшифровки (с помощью анализа SNI и данных сертификата). База данных контент-фильтра должна обновляться автоматически не реже одного раза в 24 часа.

Программный комплекс должен обеспечивать защиту компьютеров от атак из Интернет с использованием технологии NAT и межсетевого экрана с контролем состояние соединений. Должна быть предусмотрена возможность блокирование ip-адресов и протоколов по заданным условиям. Защита от сканеров сети, защита от DoS-атак и блокирование чрезмерной активности. Фильтрация нежелательной почты (спам). Возможность ограничения трафика по типу, протоколам и портам. Защита от подстановки IP адреса, при авторизации через VPN и PPPoE каждому пользователю назначается личный IP-адрес. Ограничение скорости Интернет-трафика для отдельных пользователей, компьютеров или протоколов. DNAT portmapper. Возможность прозрачной переадресации адресов и портов на другой адрес.

Система должна обеспечивать возможность доступа сотрудников к внутренней локально-вычислительной сети посредством удаленного подключения по защищенному каналу через сеть Интернет. Должна быть реализована возможность объединить все удаленные подразделения в общую сеть на единой платформе по шифрованным протоколам VPN PPTP, L2TP/IPSec, IKEv2/IPSec, SSTP, с возможностью создать закрытые корпоративные серверы для ограниченного круга сотрудников.

Система должна обеспечивать возможность ограничения полосы пропускания до Интернет-ресурсов (шейпера трафика) для пользователей и групп.

Система должна обеспечивать возможность интеграции с SIEM-системами по протоколу syslog, системами мониторинга по SNMP, DLP-системами по протоколу ICAP.

Программный комплекс должен включать в свой состав следующие интегрированные Интернет службы:

- службу предотвращения вторжений, анализирующую трафик на всех интерфейсах сервера, блокирующую опасный трафик и атаки на сервер, сохраняющий информацию о заблокированном трафике и предупреждения в логах на срок не менее трех месяцев;
- службу контроля приложений с возможностью ограничения трафика приложений (не менее чем 100 приложений с помощью DPI, включая торрент-клиенты, Skype, TeamViewer, TikTok, WhatsApp, DNSoverHTTPS, Mining (криптовалюты Bitcoin, Monero, ZCash, Ethereum));
- обратный прокси-сервер для публикации веб-ресурсов с возможностью публикации и защиты HTTP и HTTPS-сайтов;
- сконфигурированный и настроенный почтовый сервер с фильтрацией спама. Почтовый ящик должен создаваться автоматически при добавлении пользователя. Должна осуществляться поддержка нескольких почтовых доменов, доверенных сетей и доменов. Должна быть предусмотрена поддержка протокола IMAP, защищенного протокола STARTTLS и общих почтовых папок. Должна быть предусмотрена блокировка попыток подбора паролей ко всем сервисам почты. Должен быть реализован полнофункциональный веб-интерфейс для работы с личной почтой, позволяющий работать с почтой из любой точки мира по зашифрованному каналу через обычный браузер. Должны быть реализованы возможности, переадресации, групповой рассылки, фильтрации по адресам и содержанию, установка размера почтового ящика и размера письма, дублирования всей почты на один адрес, для контроля и архивирования корреспонденции, загрузки почту с других серверов по протоколам, настраиваемый автоответчик;
- полнофункциональный DNS-сервер с возможностью поддержки DNS-зон и кеширования DNS-запросов из локальной сети. С возможностью перехвата запросов на внешние DNS-сервера и принудительного разрешения доменных имен через встроенный сервер.
- DHCP-сервер для автоматического распределения IP адресов в локальной сети, обеспечивающий возможность: фиксированной привязки IP к MAC адресу компьютера; выдачи DNS и WINS для dhcp клиентов; выдачи маршрутов для DHCP клиентов; указания разных диапазонов на разных интерфейсах и VLAN.

Подписка на 12 месяцев должна включать в себя:

- Право на получение обновлений программы для ЭВМ (возможность получать новые версии продукта, обновление сигнатур);
- Право на получение технической поддержки программы для ЭВМ;
- Право использования модуля предотвращения вторжений (возможность использовать модуль и получать его обновления);
- Право использования модуля по контролю приложений (возможность использовать модуль и получать его обновления);
- Право использования модуля по фильтрации контента (возможность использовать модуль и получать его обновления).

Право использования программы для ЭВМ осуществляется в следующих пределах и способами:

- воспроизведение программы для ЭВМ в соответствии с его назначением, ограниченное правом инсталляции, копирования, запуска и хранения в памяти ЭВМ;
- осуществление настройки программы для ЭВМ в соответствии с его назначением, не представляющих собой изменение программы для ЭВМ;
- запрещено предоставлять право использования программы для ЭВМ третьим лицам, в частности, путем предоставления доступа и/или передачи электронного ключа;
- осуществление использования программы для ЭВМ на территории России и стран СНГ.

Цена должна быть указана с учетом затрат на уплату налогов и других видов сборов.

В комплект поставки должны входить:

Оптический носитель информации (CD ROM) с размещёнными на нём программным обеспечением межсетевого экрана;

Защитный пластиковый футляр для хранения оптического носителя информации;

Вкладыш в защитный пластиковый футляр для хранения оптического носителя информации;

Документированными материалами в составе: руководство администратора защиты, регламент обновления программного обеспечения МЭ

Формуляр в печатном виде;

Копия сертификата соответствия.