Утверждаю
Генеральный менеджер

_____ А.Ю. Швейн

«__08__» ноября 2017 г.

Согласовано
Член Правления,
Директор Департамента комплексной безопасности

_____ А.В. Сончик

«____» _____ 2017 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на поставку межсетевого экрана Palo Alto 3020

Лот №1

1. **Общие сведения:** поставка межсетевого экрана Palo Alto 3020.
2. **Назначение:** защита сегментов локальной вычислительной сети ПАО «ГК «Космос» от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети.
3. **Технические требования к оборудованию:**
   - Пропускная способность межсетевого экрана (при включенном APP-ID) –2 Гбит/с
   - Пропускная способность при предотвращении угроз – 1 Гбит/с
   - Пропускная способность IPSec VPN – 500 Мбит/с
   - Число новых сеансов в секунду – 16 000
   - Максимальное количество сеансов – 250 000
   - Число IPSec VPN туннелей/тунельных интерфейсов – 1 000
   - Число одновременных пользователей – GlobalProtect (SSL VPN) – 1 000
   - Число сеансов расшифровки SSL -1 000
   - Число входящих сертификатов SSL – 25
   - Число виртуальных маршрутизаторов – 10
   - Число виртуальных систем (база/макс) – 1/6
   - Число зон безопасности – 40
   - Максимальное число политик – 2 500
   - Использование чипов FPGA в архитектуре решения
   - Наличие разнесенных на аппаратном уровне data- и security plane с отдельными вычислительными мощностями на каждый из компонентов
   - Возможность использование любого из интерфейсов устройства для подключения в режимах L1, L3, L4, tap

Сенончин

4. **Требования к функционалу системы:** МЭ должен выполнять следующие основные функции:
   - обеспечение фильтрации входящего и исходящего сетевого трафика на сетевом, транспортном и прикладном уровнях на основе заданных правил фильтрации;
   - регистрация и учет фильтруемых входящих и исходящих пакетов (данных) коммуникационных протоколов сетевого уровня с указанием атрибутов фильтруемых пакетов, времени, результата фильтрации и др.;
   - идентификация и аутентификация входящих и исходящих запросов на установление соединений (протокольных блоков данных коммуникационных протоколов транспортного уровня);
   - фильтрация запросов на установление соединений на основе заданных правил фильтрации;
   - регистрация и учет фильтруемых входящих и исходящих запросов на установление соединений с указанием атрибутов фильтруемых пакетов, времени, результата фильтрации и др.;
   - обеспечение трансляции на транспортном и прикладном уровнях (прокси) для определенных протоколов;
   - регистрация и учет попыток нарушения заданных в МЭ правил фильтрации;
   - регистрация и учет входа/выхода в систему/из системы МЭ с указанием атрибутов субъекта, результата регистрируемого события и др.;
   - контроль и анализ легитимности действий, выполняемых с административными полномочиями;
   - контроль целостности программной части МЭ;
   - фильтрация вредоносного и шпионского ПО;
   - обнаружение вторжений, блокирование и предотвращение внешних атак;
   - возможность реализации функционала защиты от угроз нулевого дня в облаке разработчика или на отдельном устройстве
   - возможность интеграции репутационной базы URL и проприетарной песочницы разработчика
   - возможность интеграции функционала защиты от угроз нулевого дня и защиты рабочих станций
   - проверка траффика в один проход без использования дополнительных модулей для повторной проверки
   - возможность построения VPN посредством портала на устройстве с использованием агентов, наличие безагентного способа подключения удаленных пользователей, возможность двухфакторной аутентификации пользователей при удаленном подключении

8. **Иные требования:**

Проведение обучения специалистов с обязательной последующей сертификацией по программе:

Модуль 1: Обзор платформ и архитектуры
- Обзор платформ безопасности
- Архитектура обеспечения проверки за один проход
- Модель безопасности Zero Trust
- Безопасность облачных сервисов общего доступа
- Аппаратные и виртуальные платформы

Модуль 2: Первоначальная настройка устройства

- Графическая среда управления, командная строка и API
- Первоначальный доступ к системе
- Управление конфигурацией
- Установка обновлений операционной системы и программ, лицензирование
- Управление учетными записями администраторов
- Просмотр и фильтрация логов
- Лабораторная работа — Первоначальная настройка

Модуль 3: Настройка интерфейсов

- Зоны (Security Zones) и интерфейсы
- Типы интерфейсов — L2, L3, Virtual Wire, Tap, VLAN, loopback
- Сабинтерфейсы
- Виртуальные маршрутизаторы
- Маршрутизация на основе политик (Policy Based Forwarding)
- Лабораторная работа — Настройка интерфейсов

Модуль 4: Политики безопасности и адресной трансляции

- Базовые концепции политики безопасности
- Настройка трансляции адреса источника (Source NAT)
- Настройка трансляции адреса получателя (Destination NAT)
- Лабораторная работа — Политика безопасности

Модуль 5: Идентификация приложений (App-ID)

- Процесс идентификации приложений
- Использование приложений в политике безопасности
- Идентификация неизвестных приложений
- Обновление сигнатур приложений
- Лабораторная работа — Основы идентификации приложений

Модуль 6: Идентификация контента (Content-ID)

- Обзор механизмов идентификации контента
- Защита от атак на уязвимости
- Антивирус
- Защита от программ-шпионов
- Блокирование передачи файлов
- Использование идентификации контента в политике безопасности
- Телеметрия и анализ угроз
- Профайлы защиты зон
- Защита от DoS атак
- Лабораторная работа — Идентификация контента

Модуль 7: Фильтрация URL

- Профайлы фильтрации URL
- Применение профайлов в политике безопасности
- Лабораторная работа — Фильтрация URL

Модуль 8: Расшифровка

- Концепции расшифровки SSL
- Работа с сертификатами
- Расшифровка исходящего SSL трафика
- Расшифровка входящего SSL трафика
- Дополнительные настройки — неподдерживаемые приложения, зеркалирование трафика, отладка и исправление неполадок
- Лабораторная работа — Расшифровка SSL трафика

Модуль 9: WildFire
- Концепции WildFire
- Настройка и управление WildFire
- Отчеты WildFire
- Лабораторная работа - WildFire

Модуль 10: Идентификация пользователей
- Обзор механизма идентификации пользователей
- Методы сопоставления пользователей с адресами
- Настройка идентификации пользователей
- Настройка встроенного агента идентификации
- Настройки агента идентификации под Windows
- Соотнесение пользователей с группами
- Использование учетных записей в политике безопасности
- Лабораторная работа — Идентификация пользователей

Модуль 11: GlobalProtect
- Обзор технологии Global Protect
- Подготовка межсетевого экрана к использованию Global Protect
- Настройка портала
- Настройка шлюза
- Настройка агентов
- Лабораторная работа — Global Protect

Модуль 12: IPSec VPN
- Обзор технологии IPSec
- Построение туннеля между двумя межсетевыми экранами
- Отладка IPSec туннелей
- Лабораторная работа — Построение IPSec туннеля

Модуль 13: Мониторинг и построение отчетов
- Работа с закладками Dashboard, ACC и Monitor
- Перенаправление логов на внешние сервера
- Использование syslog
- Настройка SNMP
- Лабораторная работа — Мониторинг и построение отчетов

Модуль 14: Отказоустойчивость (High Availability, HA)
- Компоненты и функционирование HA
- Настройка режима Active/Passive

- Мониторинг состояния HA
- Лабораторная работа — High Availability

Модуль 15: Дополнительные возможности и настройки
- Рекомендации по настройке и применению
- Анализ информации в закладке ACC
- Оптимизация профайлов защиты

Срок поставки оборудования – 15 рабочих дней, начиная с даты подписания договора.

Лот №2

9. Техподдержка и дополнительные подписки

Стоимость техподдержки:

Наименование позиции	**Функционал**	**Стоимость**
Техническая поддержка Partner enabled premium support year 1, PA-3020	Замена неисправного оборудования, техническая поддержка, обновление программного обеспечения сроком на 1 год	
Техническая поддержка Partner enabled premium support 3 year prepaid, PA-3020	Замена неисправного оборудования, техническая поддержка, обновление программного обеспечения сроком на 3 года	

Стоимость обязательных дополнительных подписок:

Подписка Threat prevention subscription year 1, PA-3020	Модуль обнаружения вторжений, модуль предотвращения вторжений, модуль антивирусной защиты, модуль защиты от шпионского ПО, модуль защиты от бот-сетей. Срок действия сервиса – 1 год	
Подписка Threat prevention subscription 3-year prepaid, PA-3020	Модуль обнаружения вторжений, модуль предотвращения вторжений, модуль антивирусной защиты, модуль защиты от шпионского ПО, модуль защиты от бот-сетей. Срок действия сервиса – 3 года	

Подписка WildFire subscription year 1, PA-3020	Модуль защиты от угроз нулевого дня, модуль проверки фишинговых ссылок, которые не содержатся в репутационной базе устройства. Срок действия – 1 год	
Подписка WildFire subscription year 1, PA-3020	Модуль защиты от угроз нулевого дня, модуль проверки фишинговых ссылок, которые не содержатся в репутационной базе устройства. Срок действия – 3 года	

Стоимость желательных дополнительных подписок:

Подписка PANDB URL filtering subscription year 1, PA-3020	Модуль проверки ресурсов сети интернет, модуль проверки ссылок в электронной почте, модуль проверки фишинговых ссылок. Проприетарная база разработчика. Срок действия – 1 год	
Подписка PANDB URL filtering subscription 3-year prepaid, PA-3020	Модуль проверки ресурсов сети интернет, модуль проверки ссылок в электронной почте, модуль проверки фишинговых ссылок. Проприетарная база разработчика. Срок действия – 3 года	

Руководитель направления по ИБ и ТСО
В. Гаргосов
vgargosov@hotelcosmos.ru
+79859153979