Приложение № 1 к извещению

**ОПИСАНИЕ ОБЪЕКТА ЗАКУПКИ (ТЕХНИЧЕСКОЕ ЗАДАНИЕ)**

**НА ПОСТАВКУ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

**Содержание**

[1 Общие требования 3](#_Toc111046965)

[2 Требования к Криптошлюзу 4](#_Toc111046966)

[2.1 Функциональные требования 4](#_Toc111046967)

[2.2 Требования к аппаратной части 6](#_Toc111046968)

[3 Требования к ПАК МЭ и СОВ 7](#_Toc111046969)

[3.1 Функциональные требования 7](#_Toc111046970)

[3.2 Требования к аппаратной части 8](#_Toc111046971)

# Общие требования

Настоящий документ содержит технические требования к средствам защиты информации:

* ПАК ViPNet Coordinator HW1000 (Криптошлюз);
* ПАК ViPNet xFirewall 1000 D, объединяющий в себе функции межсетевого экрана (далее – МЭ) и системы обнаружения (предотвращения) вторжений (далее – СОВ).

Все оборудование должно поставляться в комплекте с документацией, копиями сертификатов соответствия (в электронном виде на компакт-диске) и формулярами (в бумажном виде), заверенными печатью фирмы-производителя.

Все оборудование должно быть новым (ранее не использованным), предназначенным для использования в составе защищенной сети Заказчика № 1100.

В состав поставки должны входить:

* Кластер из двух ПАК ViPNet Coordinator HW1000 – 3 шт.
* Кластер из двух ПАК ViPNet xFirewall 1000 D – 3 шт.

Требования к гарантийному сроку: 12 (двенадцать) месяцев с даты подписания Заказчиком документа о приемке.

Получатель: Государственное учреждение – Ростовское региональное отделение Фонда социального страхования Российской Федерации

Место поставки: 344082, г. Ростов-на-Дону, ул. Красноармейская, д. 36/62

Срок поставки: до 15 календарных дней с даты подписания государственного контракта.

ОКПД2 26.20.40.140

# Требования к Криптошлюзу

## Функциональные требования

Криптошлюз должен обеспечивать:

* построение VPN-сети, позволяющей организовать одно или множество сетевых соединений (логическую сеть) поверх каналов связи сетей передачи данных, использующих протоколы семейства TCP/IP;
* криптографическую защиту данных (шифрование, аутентификацию, защиты от повторов и изменений), передаваемых по каналам VPN;
* возможность организации в одном устройстве защищенного соединения как на сетевом, так и канальном уровне модели OSI;
* регистрацию информации о текущих и виртуальных IP-адресах узлов VPN-сети;
* возможность объединения до 30 сегментов локальной вычислительной сети (далее – ЛВС) на канальном уровне модели OSI;
* установление каналов VPN между клиентами в защищенных сетях и удаленными клиентами VPN через межсетевые экраны и устройства с NAT;
* возможность подключения клиентов VPN по протоколам TCP при недоступности UDP;
* контроль и фильтрацию проходящих через сетевые интерфейсы Криптошлюза информационных потоков данных в соответствии с заданными правилами;
* реализацию функций прокси-сервера с возможностью фильтрации HTTP-трафика по его содержимому;
* трансляцию IP-адресов и портов (SNAT/DNAT);
* обработку прикладных протоколов FTP, DNS, H.323, SCCP, SIP для всех видов трафика (защищенного, открытого и туннелируемого);
* статическую маршрутизацию;
* динамическую маршрутизацию средствами протокола OSPF;
* предоставление DHCP-, DNS-, NTP-сервисов защищаемым сетевым объектам;
* построение виртуальных локальных сетей (поддержка стандарта VLAN IEEE 802.1 Q);
* поддержку технологии агрегирования – объединения нескольких физических каналов передачи данных в сетях Ethernet в один логический;
* балансировку нагрузки на вычислительную сеть и резервирование каналов доступа во внешнюю сеть средствами функции MultiWAN, включающую в себя проверку состояния Криптошлюза (DGD) и политики маршрутизации;
* возможность антивирусной защиты HTTP-трафика при взаимодействии по протоколу ICAP с внешним средством антивирусной защиты, сертифицированным на соответствие требованиям ФСБ России и (или) ФСТЭК России;
* возможность изменения значения MTU для сетевых интерфейсов;
* обеспечения политики качества обслуживания (QoS) приоритетной обработки средствами сервиса дифференцированного обслуживания (DiffServ);
* взаимодействие с источником бесперебойного питания (UPS) для корректного завершения работы в случае получения сигнала об истощении батареи;
* замкнутость и контроль целостности среды функционирования;
* удаленное (защищенное) управление и мониторинг с помощью веб-интерфейса и SSH;
* сигнализацию о событиях в системе мониторинга по протоколам SNMP, syslog;
* удаленное обновление собственного ПО;
* возможность кластеризации с целью обеспечения горячего резервирования.

Криптошлюз должен соответствовать требованиям:

* ФСБ России к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса KC3;
* документов «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016).

## Требования к аппаратной части

Криптошлюз должен удовлетворять следующим требованиям:

* форм-фактор – 1U;
* наличие не менее 4 (четырех) сетевых интерфейсов Ethernet RJ45 10/100/1000 Мбит/с.

# Требования к ПАК МЭ и СОВ

## Функциональные требования

ПАК МЭ и СОВ должен обеспечивать:

* фильтрацию трафика на сетевом и транспортном уровнях модели OSI по адресу источника, адресу назначения, протоколам и портам;
* фильтрацию трафика на прикладном уровне модели OSI с помощью технологии расширенной инспекции содержимого трафика сетевых приложений;
* трансляцию сетевых адресов (SNAT/DNAT);
* обработку прикладных протоколов FTP, H.323, SCCP, SIP;
* возможность построения виртуальных локальных сетей (поддержку стандарта VLAN IEEE 802.1 Q);
* поддержку технологии агрегирования – объединения нескольких физических каналов передачи данных в сетях Ethernet в один логический);
* реализацию функции DHCP-, DNS-, NTP-сервера и агента DHCP-relay;
* статическую маршрутизацию;
* динамическую маршрутизацию средствами протокола OSPF;
* реализацию политики качества обслуживания (QoS) приоритетной обработки средствами сервиса дифференцированного обслуживания (DiffServ);
* возможность кластеризации с целью обеспечения горячего резервирования;
* взаимодействие с источником бесперебойного питания (UPS) для корректного завершения своей работы в случае получения сигнала об истощении батареи;
* поддержку нескольких контроллеров домена;
* диагностику основных параметров ПАК МЭ и СОВ по протоколу SNMP;
* фильтрацию HTTP-трафика интегрированным прокси-сервером и его антивирусную проверку встроенным или внешним (по протоколу ICAP) антивирусами;
* обнаружение и блокирование сетевых вторжений на основе анализа трафика сигнатурным и эвристическим методами с использованием базы правил, содержащей описания сетевых угроз в специальном формате (правила IPS);
* автоматизированное обновление базы решающих правил;
* сигнализацию о событиях по протоколам snmp, syslog;
* удаленное обновление программного обеспечения;
* удаленное управление и мониторинг функционирования ПАК МЭ и СОВ с помощью веб-интерфейса и SSH.

ПАК должен соответствовать требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020)» - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты ИТ.МЭ.А4.ПЗ» (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 к аппаратной части

ПАК МЭ и СОВ должен удовлетворять следующим требованиям:

* форм-фактор –1U;
* наличие не менее 4 (четырех) сетевых интерфейсов Ethernet RJ45 10/100/1000 Мбит/с;
* наличие не менее 2 (двух) сетевых интерфейсов Ethernet SFP 1 Гбит/с.