МІНІСТЭРСТВА АХОВЫ ЗДАРОЎЯ
РЭСПУБЛІКІ БЕЛАРУСЬ
ГОМЕЛЬСКАЕ
ГАНДЛЕВА-ВЫТВОРЧАЕ
РЭСПУБЛІКАНСКАЕ
УНІТАРНАЕ ПРАДПРЫЕМСТВА
«ФАРМАЦЫЯ»
246027 г. Гомель, вул. Мазырская, 16А
Факс: 40-06-72;Email:farm@mail.gomel.by

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ БЕЛАРУСЬ
ГОМЕЛЬСКОЕ
ТОРГОВО-ПРОИЗВОДСТВЕННОЕ
РЕСПУБЛИКАНСКОЕ
УНИТАРНОЕ ПРЕДПРИЯТИЕ
«ФАРМАЦИЯ»
246027 г. Гомель, ул. Мозырская, 16А
Факс: 40-06-72;Email:farm@mail.gomel.by

Генеральный директор	**29-27-77**
Зам. генерального директора	**29-23-00**
Приёмная	**29-20-19**
Отдел организации медснабжения	**29-21-98**
Отдел маркетинга и внешнеэкономических отношений	**29-22-16**
Отдел организации бухгалтерского учёта, отчётности и контроля	**29-23-89**

17.08.2026 № 09-57/4194

Руководителю организации

Заявка на изучение
конъюнктуры рынка

В связи с планируемым осуществлением закупки за счет собственных средств в соответствии с постановлением Совета Министров Республики Беларусь от 07.04.2026 № 168 «О закупках товаров (работ, услуг) за счет собственных средств», Гомельское торгово-производственное республиканское унитарное предприятие проводит изучение конъюнктуры рынка для определения исполнителя (поставщика) и формирования ориентировочной стоимости закупки.

Просим Вас рассмотреть прилагаемое техническое задание и направить в наш адрес ценовое предложение (farm@mail.gomel.by или 246027, г. Гомель, ул. Мозырская, 16А).

Предмет закупки: Комплект оборудования криптографической защиты информации с установкой и настройкой защищённой корпоративной сети передачи данных.

Условия оплаты: в четыре этапа (предоплата 30% в течение 5 банковских дней с момента заключения договора; вторая часть 30% в срок до 31.10.2026; третья часть 20% в срок до 30.11.2026; четвертая часть 20 % в срок до 20.12.2026).

Условия и место поставки: доставка транспортом Поставщика по адресу г. Гомель, ул. Мозырская, 16А).

Срок поставки оборудования: в течение 30 календарных дней с момента подписания договора.

Валюта цены: белорусский рубль (BYN). Цена должна включать все расходы Поставщика, в том числе транспортные расходы, налоги, сборы и другие обязательные платежи (указать с НДС или без НДС).

Страна происхождения товара: просим обязательно указать страну происхождения предлагаемой продукции, а также статус Вашей

организации (является ли организация производителем, официальным торговым представителем или иное).

Ваше ценовое предложение просим направить в наш адрес в срок не позднее 15:00 21.08.2026 на электронную почту farm@mail.gomel.by с пометкой «Ценовое предложение на закупку» или по адресу 246027, г. Гомель, ул. Мозырская, 16А.

Настоящий запрос не является приглашением к участию в конкурентной процедуре закупок, не признается офертой и не влечет за собой возникновения каких-либо обязательств со стороны Заказчика по заключению договора.

Приложение: Техническое задание

Заместитель
генерального директора В.А.Крюк

11 Курлович 224124

УТВЕРЖДАЮ
Генеральный директор
Гомельского УП «Фармация»
_____ Л.А. Сапего
«____» _____ 2026 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на поставку оборудования и выполнение работ по созданию защищённой корпоративной сети передачи данных

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и цель закупки

Настоящее техническое задание (далее — ТЗ) определяет требования к поставке оборудования и выполнению работ по созданию защищённой корпоративной сети передачи данных (далее — КСПД) с применением средств криптографической защиты информации (далее — СКЗИ) белорусского производства и межсетевых экранов нового поколения (далее — NGFW).

2. СОСТАВ ЗАКУПКИ. ПЕРВАЯ ОЧЕРЕДЬ

Закупка осуществляется по позициям, указанным в разделах 3–6 настоящего ТЗ. Все позиции объединены в одну закупку. Частичное исполнение не допускается.

2.1 Сводная таблица закупаемых позиций

№	Наименование	Кол-во	Единица
1	Коммутатор уровня агрегации L3, 48×1GbE, аплинки 2×40G + 4×25G, резерв. БП	2	шт.
2	Кабель DAC SFP+ 2 м	8	шт.

3	Услуга по установке и настройке коммутаторов агрегации (поз. 1)	1	шт.
4	Кластер NGFW тип 1 Active/Passive, 2 ПАК + лицензии + ТП 1 год	1	компл.
5	Услуга по установке и настройке NGFW тип 1	1	шт.
6	ПАК СКЗИ тип 1, производительность до 10 Гбит/с, лицензия неогр. тун.	2	шт.
7	Услуга по установке и настройке СКЗИ тип 1	1	шт.
8	Сервер управления и приложений	1	шт.
9	Услуга по установке и настройке сервера	1	шт.
10	Коммутатор ядра L3, 12×10G SFP+, 8×25G SFP28, 2×40G, резерв. БП	2	шт.
11	Коммутатор доступа L3, 24×1GbE, аплинки 2×40G + 4×25G, резерв. БП	3	шт.
12	Коммутатор доступа L3, 48×1GbE, аплинки 2×40G + 4×25G, резерв. БП	4	шт.
13	Кабель DAC SFP+ 2 м	6	шт.
14	Коммутатор доступа L2+ 8*10/100/1000Base-T PoE 802.3af/at + 2*1000/2500Base-X SFP, дальность до 250м, 120Вт	5	шт.
15	Услуга по установке и настройке коммутаторов (поз. 10, 11, 12, 14)	1	шт.
16	Кластер NGFW тип 2: Active/Passive, 2 ПАК + лицензии + ТП 1 год	1	компл.
17	Услуга по установке и настройке NGFW тип 2	1	шт.

18	ПАК СКЗИ тип 2 (Склад), производительность до 100 Мбит/с, лицензия до 10 тун.	2	шт.
19	Услуга по установке и настройке СКЗИ тип 2	1	шт.
20	Коммутатор доступа L2/L3, 24×1GbE, 4×10G SFP+	24	шт.
21	Услуга по установке и настройке коммутаторов (поз. 20)	1	шт.
22	ПАК СКЗИ тип 2, производительность до 100 Мбит/с, лицензия до 10 тун.	24	шт.
23	Услуга по установке и настройке СКЗИ тип 2	1	шт.
24	Шкаф телекоммуникационный настенный 12U в сборе с комплектующими	24	компл.
25	Услуга по сборке и установке шкафов (поз. 24)	1	шт.
26	Активный Кабель DAC QSFP 40G 1 м	4	шт.

3. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К СКЗИ

3.1 ПАК СКЗИ тип 1 — Шлюз криптографической защиты (Hub), производительность до 10 Гбит/с, лицензия на неограниченное количество туннелей шифрования

Количество: 2 шт. (для установки в режиме Active/Standby)

Поставляемый ПАК должен соответствовать следующим требованиям:

3.1.1. Имеет действующий сертификат соответствия требованиям технического регламента ТР 2013/027/BY.

3.1.2. Обеспечивает криптографическую защиту передаваемых данных посредством полной инкапсуляции IP-пакетов (IPsec VPN в туннельном режиме).

3.1.3. Обеспечивает подключение к 100/1000 Мбит/с Ethernet IEEE 802.3 порту IP-сети и имеет не менее 4 сетевых интерфейсов (RJ45).

3.1.4. Количество портов 10GBASE-R (SFP+) не менее 2.
3.1.5. Наличие интерфейса для удалённого управления и мониторинга аппаратной части ПАК.
3.1.6. Объём твердотельного накопителя: не менее 240 Гигабайт.
3.1.7. Производительность шифрования – до 5,2 Гбит/с (размер пакета (MTU) 1500, 33 vCPU), до 9,7 Гбит/с (MTU 8838, 39 vCPU) на TCP-трафике;
3.1.8. Количество одновременно поддерживаемых VPN-туннелей – неограниченное количество туннелей;
3.1.9. Все поставляемые с ПАК лицензии являются бессрочными.
3.1.10. Процессор аппаратной платформы должен соответствовать требованиям:

- линейка не ниже Intel Gold;
- обязательно поддерживать инструкции RDRAND и RDSEED.

3.1.11. Соответствие СТБ 34.101.27.2022 (уровень 3).
3.1.12. Поддерживает алгоритмы шифрования согласно СТБ 34.101.31-2020.
3.1.13. Поддерживает алгоритмы вычисления хэш-значений согласно СТБ 34.101.31-2020.
3.1.14. Поддерживает алгоритмы контроля целостности (вычисления имитовставки) согласно СТБ 34.101.31-2020.
3.1.15. Поддержка алгоритмов электронной-цифровой подписи согласно СТБ 34.101.45-2013.
3.1.16. Поддерживает процедуру выработки псевдослучайных чисел в соответствии с п.5.10 СТБ 34.101.27-2022.
3.1.17. Поддержка протоколов защиты трафика IPsec Encapsulating Security Payload (ESP) и IPsec Authentification Header (AH).
3.1.18. Поддержка режима IKE-CFG для объединения различных сетевых объектов в виртуальную локальную сеть с назначением IP-адресов из локального пула.
3.1.19. Поддерживает режим аутентификации устройств IKE с использованием технологических сертификатов открытого ключа по СТБ 34.101.45-2013.

3.1.20. Поддерживает аутентификации устройств IKE по «preshared key».

3.1.21. Поддерживает аутентификацию устройств с использованием технологических сертификатов открытого ключа УЦ ГосСУОК, с возможностью фильтрации доступа по полям субъекта сертификата.

3.1.22. Поддержка проверки цепочки сертификатов доверенных УЦ.

3.1.23. Поддерживает протокол NAT Traversal IPsec.

3.1.24. Поддержка функционала межсетевого экрана согласно СТБ 34.101.73-2017.

3.1.25. Обеспечивает надежность защищенных соединений с помощью протокола DPD.

3.1.26. Формат сертификатов открытых ключей X.509 v.3 согласно СТБ 34.101.19-2012.

3.1.27. Поддерживает ведения журнала событий безопасности по протоколу Syslog.

3.1.28. Поддерживает статическую и динамическую маршрутизацию (RIPv2, OSPF).

3.1.29. Поддерживает получение статистики по протоколу SNMP v.1, v.2c.

3.1.30. Поддерживает технологию VRRP и RRI для обеспечения отказоустойчивости.

3.1.31. Позволяет осуществлять фильтрацию по IP-адресу (диапазон IP, хост) источника и назначения, по порту и типу протокола.

3.1.32. Авторизационное письмо о совместимости от производителя продуктов Bel VPN компании ООО "С-Терра Бел" со следующими продуктами:

- КПА «Шлюз BelVPN 4.7»;
- ПАК «Шлюз безопасности «Bel VPN Gate 4.5»;
- ПАК «Шлюз безопасности «Bel VPN Gate 4.1»;
- ПК «Шлюз безопасности «Bel VPN Gate 4.5»;
- ПК «Шлюз безопасности виртуальный «Bel VPN Gate-V 4.1»;
- ПП «Клиент безопасности «Bel VPN Client-P 4.1»;

- ПП «Клиент безопасности «Bel VPN Client 4.5»;
- ПП «Клиент безопасности мобильный «Bel VPN Client-M 4.5»;
- ПП «Шлюз BelVPN 4.7».

3.1.33. Наличие декларации соответствия технического регламента таможенного союза «О безопасности низковольтного оборудования» (ТР ТС 004/2011) КПА «Шлюз BelVPN 4.7;

3.1.34. Наличие декларации соответствия технического регламента таможенного союза «Электромагнитная совместимость технических средств» (ТР ТС 020/2011) КПА «Шлюз BelVPN 4.7;

3.1.35. Наличие сертификата соответствия требованиям системы менеджмента качества СТБ ISO 9001-2015;

3.1.36. Наличие сертификата соответствия требованиям системы менеджмента информационной безопасности СТБ ISO/IEC 27001-2024;

3.2 ПАК СКЗИ тип 2 — Шлюз криптографической защиты (узловой), производительность до 100 Мбит/с, лицензия до 10 туннелей шифрования

Количество: 26 шт.

Поставляемый ПАК должен соответствовать следующим требованиям:

3.2.1. Имеет действующий сертификат соответствия требованиям технического регламента ТР 2013/027/BY.

3.2.2. Обеспечивает криптографическую защиту передаваемых данных посредством полной инкапсуляции IP-пакетов (IPsec VPN в туннельном режиме).

3.2.3. Обеспечивает подключение к 100/1000 Мбит/с Ethernet IEEE 802.3 порту IP-сети и имеет не менее 4 сетевых интерфейсов (RJ45).

3.2.4. Производительность шифрования – до 100 Мб/с на TCP-трафике;

3.2.5. Количество одновременно поддерживаемых VPN-туннелей – 10 туннелей;

3.2.6. Все поставляемые с ПАК лицензии являются бессрочными.

3.2.7. Процессор аппаратной платформы должен соответствовать требованиям:

- линейка не ниже Intel Celeron(архитектура Broadwell);
- обязательно поддерживать инструкции RDRAND и RDSEED.

3.2.8. Соответствие СТБ 34.101.27.2022 (уровень 3).

3.2.9. Поддерживает алгоритмы шифрования согласно СТБ 34.101.31-2020.

3.2.10. Поддерживает алгоритмы вычисления хэш-значений согласно СТБ 34.101.31-2020.

3.2.11. Поддерживает алгоритмы контроля целостности (вычисления имитовставки) согласно СТБ 34.101.31-2020.

3.2.12. Поддержка алгоритмов электронной-цифровой подписи согласно СТБ 34.101.45-2013.

3.2.13. Поддерживает процедуру выработки псевдослучайных чисел в соответствии с п.5.10 СТБ 34.101.27-2022.

3.2.14. Поддержка протоколов защиты трафика IPsec Encapsulating Security Payload (ESP) и IPsec Authentification Header (AH).

3.2.15. Поддержка режима IKE-CFG для объединения различных сетевых объектов в виртуальную локальную сеть с назначением IP-адресов из локального пула.

3.2.16. Поддерживает режим аутентификации устройств IKE с использованием технологических сертификатов открытого ключа по СТБ 34.101.45-2013.

3.2.17. Поддерживает аутентификации устройств IKE по «preshared key».

3.2.18. Поддерживает аутентификацию устройств с использованием технологических сертификатов открытого ключа УЦ ГосСУОК, с возможностью фильтрации доступа по полям субъекта сертификата.

3.2.19. Поддержка проверки цепочки сертификатов доверенных УЦ.

3.2.20. Поддерживает протокол NAT Traversal IPsec.

3.2.21. Поддержка функционала межсетевого экрана согласно СТБ 34.101.73-2017.

3.2.22. Обеспечивает надежность защищенных соединений с помощью протокола DPD.

3.2.23. Формат сертификатов открытых ключей X.509 v.3 согласно СТБ 34.101.19-2012.

3.2.24. Поддерживает ведения журнала событий безопасности по протоколу Syslog.

3.2.25. Поддерживает статическую и динамическую маршрутизацию (RIPv2, OSPF).

3.2.26. Поддерживает получение статистики по протоколу SNMP v.1, v.2c.

3.2.27. Поддерживает технологию VRRP и RRI для обеспечения отказоустойчивости.

3.2.28. Позволяет осуществлять фильтрацию по IP-адресу (диапазон IP, хост) источника и назначения, по порту и типу протокола.

3.2.29. Авторизационное письмо о совместимости от производителя продуктов Bel VPN компании ООО "С-Терра Бел" со следующими продуктами:

- КПА «Шлюз BelVPN 4.7»;
- ПАК «Шлюз безопасности «Bel VPN Gate 4.5»;
- ПАК «Шлюз безопасности «Bel VPN Gate 4.1»;
- ПК «Шлюз безопасности «Bel VPN Gate 4.5»;
- ПК «Шлюз безопасности виртуальный «Bel VPN Gate-V 4.1»;
- ПП «Клиент безопасности «Bel VPN Client-P 4.1»;
- ПП «Клиент безопасности «Bel VPN Client 4.5»;
- ПП «Клиент безопасности мобильный «Bel VPN Client-M 4.5»;
- ПП «Шлюз BelVPN 4.7».

3.2.30. Наличие декларации соответствия технического регламента таможенного союза «О безопасности низковольтного оборудования» (ТР ТС 004/2011) на КПА «Шлюз BelVPN 4.7»;

3.2.31. Наличие декларации соответствия технического регламента таможенного союза «Электромагнитная совместимость технических средств» (ТР ТС 020/2011) на КПА «Шлюз BelVPN 4.7;

3.2.32. Наличие сертификата соответствия требованиям системы менеджмента качества СТБ ISO 9001-2015;

3.2.33. Наличие сертификата соответствия требованиям системы менеджмента информационной безопасности СТБ ISO/IEC 27001-2024;

4. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К МЕЖСЕТЕВЫМ ЭКРАНАМ НОВОГО ПОКОЛЕНИЯ (NGFW)

4.1 Общие требования

4.1.1 Требования к составу и структуре программно-аппаратного комплекса

4.1.1.1 В состав программно-аппаратного комплекса «Межсетевой экран нового поколения» должны входить следующие компоненты:

- ПАК «Межсетевой экран» (далее также — Межсетевой экран);
- образ виртуальной машины «Модуль управления» (далее также — Модуль управления);

4.1.1.2 ПАК, входящие в состав программно-аппаратного комплекса «Межсетевой экран нового поколения», должны включать в себя:

- предустановленное специализированное программное обеспечение (далее – ПО);
- предустановленное системное ПО (операционную систему, являющуюся средой функционирования);
- аппаратные платформы общего назначения.

4.1.2 Требования к сертификации

4.1.2.1 Межсетевой экран нового поколения должен иметь действующий сертификат соответствия требованиям ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность» (СТБ 34.101.1-2014, СТБ 34.101.2-2014, СТБ 34.101.3-2014, СТБ 34.101.8-2006 (пункты 6.5, 6.8), СТБ34.101.14-2017, СТБ34.101.73-2017(пункты 7.3-7.6),СТБ34.101.75-2017 (пункты 7.2, 7.4, 7.6, 7.8)).

4.2 Комплект поставки

4.2.1 Комплект поставки

4.2.1.1 Комплект поставки должен включать следующие компоненты:

- ПАК «Межсетевой экран» тип 1 — 2 шт.;
- ПАК «Межсетевой экран» тип 2 — 2 шт.;
- образ виртуальной машины «Модуль управления» — 1 шт.

4.2.1.2 Комплект поставки должен содержать следующие лицензии:

1) базовая лицензия ПАК «Межсетевой экран» тип 1 — 2 шт.;
2) базовая лицензия ПАК «Межсетевой экран» тип 2 — 2 шт.;
3) лицензия для виртуальной машины «Модуль управления» — 1 шт.;
4) функциональные лицензии на ПАК «Межсетевой экран» тип 1:
   - единая лицензия полной функциональности продукта — 2 шт.
5) функциональные лицензии на ПАК «Межсетевой экран» тип 2:
   - единая лицензия полной функциональности продукта — 2 шт.

4.2.1.3 Срок действия поставляемых в составе ПАК «Межсетевой экран нового поколения» лицензий должен составлять 1 (один) год.

4.2.2 Требования к аппаратным платформам программно-аппаратного комплекса

4.2.2.1 Аппаратные платформы, используемые компонентами межсетевого экрана нового поколения, должны быть построены на основе платформ общего назначения на базе архитектуры центрального процессора x86.

4.2.2.2 Аппаратная платформа ПАК «Межсетевой экран» должна иметь выделенный интерфейс, обеспечивающий доступ к Модулю управления.

4.2.2.3 Трафик, поступающий на интерфейс управления, должен обрабатываться на отдельном ядре процессора, выделенным только под задачу управления. Для сохранения управляемости устройства при любых нагрузках необходимо, чтобы данное ядро процессора не должно быть задействовано под обработку основного пользовательского трафика.

4.3 Требования к программному обеспечению программно-аппаратного комплекса

4.3.1.1 В качестве системного ПО, используемого на аппаратных платформах общего назначения, должны использоваться серверные операционные системы семейства Debian не ниже версии 11 (Bullseye) или семейства Astra Linux не ниже версии 1.7, поставляемые в составе программно-аппаратного комплекса.

4.4 Требования к функциям программно-аппаратного комплекса

4.4.1 Требования к режимам сбора и перенаправления сетевого трафика

4.4.1.1 Межсетевой экран нового поколения должен иметь возможность работы в следующих режимах сетевой модели OSI:

- прозрачного моста L2 с трансляцией VLAN ID. Прозрачный мост должен формироваться как для пары физических интерфейсов, так и для пары логических подынтерфейсов (пара отдельных VLAN ID), а также комбинаций физических интерфейсов и VLAN ID. Интерфейсы прозрачного моста должны поддерживать разнесение в разные зоны безопасности;
- L3-маршрутизатора.

4.4.1.2 Межсетевой экран нового поколения в режиме L3-маршрутизатора должен поддерживать:

- статическую маршрутизацию;
- динамическую маршрутизацию;
- режим трансляции сетевых адресов (NAT).

4.4.2 Требования к фильтрации трафика

4.4.2.1 Межсетевой экран нового поколения должен поддерживать возможность формирования правил фильтрации сетевого трафика средствами Модуля управления.

4.4.2.2 Межсетевой экран нового поколения должен предоставлять возможность объединения правил фильтрации для проходящего через межсетевой экран сетевого трафика в единой политике безопасности, используя в качестве квалификаторов следующие параметры политики безопасности:

- IP-адрес(а) отправителя;
- IP-адрес(а) получателя;
- номер(а) порта(ов) для протоколов TCP и UDP, в том числе с выбором срабатывания политики только для стандартных портов протокола определяемого приложения;
- идентификатор групп пользователей подключаемого домена или идентификаторы отдельных пользователей;
- наименование приложения, генерирующего сетевой трафик, включая «Битрикс», «Яндекс Диск», WhatsApp, Telegram, OpenVPN, WireGuard;
- наименование сервиса, функции или подфункции приложения, например: загрузка файла на «Яндекс Диск», скачивание файла с «Яндекс Диска», фотографии «ВКонтакте», просмотр видео «ВКонтакте», музыка «ВКонтакте» и т. д.;
- URL-категории;
- географическая принадлежность публичного сетевого адреса назначения;
- полностью определенное доменное имя;
- время действия правила;

- идентификатор зоны безопасности, применяемой для логического разделения сетей на межсетевом экране.

4.4.2.3 Каждое правило для проходящего через межсетевой экран трафика должно поддерживать следующие режимы журналирования в выделенный компонент модуля журналирования или модуля централизованного управления:

- при срабатывании правила (до определения протокола L7/приложения);
- в начале сессии передачи данных (сразу после определения протокола L7/приложения);
- в конце сессии передачи данных;
- в начале и в конце сессии;
- периодически — до определения протокола L7/приложения и через заданный интервал времени;
- без журналирования.

4.4.3 Требования к идентификации приложений

4.4.3.1 Межсетевой экран нового поколения должен иметь возможность определения приложений прикладного уровня с помощью технологии анализа пакетов (DPI) вне зависимости от сетевых портов TCP/UDP на всем объеме инспектируемого трафика.

4.4.3.2 Межсетевой экран нового поколения должен поддерживать написание правил фильтрации трафика с использованием имени приложения прикладного уровня в качестве квалификатора.

4.4.3.3 Межсетевой экран нового поколения должен поддерживать создание политик безопасности с использованием имени сервиса, функции и подфункции приложения, включая загрузку файла на «Яндекс Диск», скачивание файла с «Яндекс Диска», фотографии «ВКонтакте», видео «ВКонтакте», музыку «ВКонтакте» и т. д.

4.4.3.4 Межсетевой экран нового поколения должен иметь возможность отображения списка и описания распознаваемых приложений в пересылаемом сетевом трафике в модуле централизованного управления.

4.4.3.5 Характеристики приложений (сигнатуры) должны содержать информацию о транспортных портах приложения (портах TCP/UDP), используемых приложением по умолчанию, для детектирования работы приложений на нестандартных портах.

4.4.3.6 Межсетевой экран нового поколения должен иметь возможность детектировать и при необходимости блокировать работу приложений на нестандартных сетевых портах TCP/UDP.

4.4.3.7 Межсетевой экран нового поколения должен поддерживать распознавание приложений прикладного уровня внутри зашифрованного трафика версии TLS 1.2, TLS 1.3.

4.4.3.8 Межсетевой экран нового поколения должен иметь возможность определения промышленных протоколов, включая BACnet, CIP, Vnet/IP, OPC UA, IEC 104, Modbus, UMAS, MMS, S7Comm и S7CommPlus.

4.4.4 Требование к функциям предотвращения вторжений

4.4.4.1 Межсетевой экран нового поколения должен обеспечивать возможность обнаружения и предотвращения вторжений, в том числе позволять:

- обнаруживать признаки компьютерных атак в проходящем через межсетевой экран трафике на основе базы сигнатур;
- автоматически блокировать сетевые взаимодействия, в которых обнаружены признаки компьютерной атаки;
- обеспечивать обновление базы решающих правил (сигнатур) с ресурсов производителя, опубликованных в сети Интернет или через службу технической поддержки производителя.

4.4.4.2 Межсетевой экран нового поколения должен иметь возможность обнаружения и предотвращения атак, таких как внедрение SQL-кода, XSS и других, при условии активированной функции предотвращения вторжений.

4.4.4.3 Межсетевой экран должен поддерживать создание профилей IPS и предоставлять возможность переопределять действие сигнатуры (блокировка или разрешение трафика), заданное производителем.

4.4.4.4 Межсетевой экран должен поддерживать уникальные профили IPS для уникальных контекстов межсетевых экранов.

4.4.4.5 Межсетевой экран нового поколения должен иметь возможность отображения списка и описания сигнатур обнаружения вторжений.

4.4.4.6 Межсетевой экран в режиме определения приложений должен запускать модуль IPS на стадии определения приложения.

4.4.5 Требования к функциям защиты от вредоносного программного обеспечения

4.4.5.1 Межсетевой экран нового поколения должен обеспечивать защиту от вредоносного программного обеспечения, в том числе позволять:

- обнаруживать признаки вредоносного программного обеспечения в проходящем через межсетевой экран трафике на основе базы данных признаков вредоносного программного обеспечения;
- блокировать сетевой трафик, в котором обнаружены признаки вредоносного программного обеспечения;
- обеспечивать обновление базы данных признаков вредоносного программного обеспечения с ресурсов производителя программно-аппаратного комплекса в сети Интернет.

4.4.5.2 Межсетевой экран нового поколения должен предоставлять возможность осуществления антивирусного контроля данных, передаваемых в зашифрованном трафике SSL/TLS-соединений.

4.4.6 Требования к URL-фильтрации

4.4.6.1 Межсетевой экран нового поколения должен предоставлять возможность блокирования доступа пользователей к интернет-ресурсам.

4.4.6.2 Межсетевой экран нового поколения должен включать обновляемую и поддерживаемую производителем на постоянной основе базу данных категорий URL.

4.4.6.3 В состав предопределенных URL-категорий должны быть включены (но не ограничиваются этим списком):

- вредоносные сайты (вредоносный контент, например: вредоносные исполняемые файлы, скрипты, вирусы, трояны или код; сайты, которые способствуют заражению через drive-by-загрузки, эксплойт-киты и т. д.);
- командные центры бот-нетов (ресурсы, на которых размещаются URL-адреса и домены сетей управления ботами (Command-and-Control). Они используются вредоносным ПО или скомпрометированными системами для скрытой связи с удаленным сервером злоумышленника, что позволяет получать вредоносные инструкции или красть данные);
- фишинг (поддельные веб-страницы, созданные для имитации настоящих сайтов компаний. Такие платформы тайно собирают конфиденциальную информацию, такую как учетные данные, номера банковских карт, PIN-коды и другие личные данные (ПДн, PII), используя методы социальной инженерии, как с согласия, так и без согласия пользователя);
- нелегальное содержимое (информация, методы или руководства по ненасильственным мошенническим или незаконным действиям, таким как аферы, подделка, уклонение от уплаты налогов, мелкие кражи, шантаж и подобные действия);
- криптомайнинг (инструменты для майнинга криптовалют и майнинговые пулы. Должна включать сайты, которые позволяют майнерам объединять свои вычислительные мощности в сети, а также сайты, которые размещают вредоносное ПО, рекламное ПО или другое нежелательное программное обеспечение, относящееся к майнингу, в том числе встроенные криптовалютные майнеры, схемы кликджекинга или программы, изменяющие настройки браузера без согласия пользователя);

- программы-вымогатели (платформы, которые размещают, распространяют или участвуют во вредоносной деятельности, связанной с программами-вымогателями. Эти кампании обычно угрожают публикацией конфиденциальных данных или блокируют доступ к определенным данным или системам, часто с помощью шифрования, до тех пор, пока не будет выплачен выкуп. Эта категория должна включать URL-адреса, распространяющие связанные с этим стилеры, вайперы и лоадеры, способные доставлять полезную нагрузку программ-вымогателей);

- социальные сети (онлайн-платформы, предназначенные для помощи пользователям в создании и поддержании социальных связей с людьми, которые имеют схожие интересы, занятия, хобби и отношения. Сайты, которые позволяют пользователям обмениваться сообщениями, фотографиями и участвовать в различных формах общения);

- поиск работы и карьера (поиск работы или найм сотрудников, включая кадровые агентства и консалтинговые услуги, предлагающие списки вакансий и возможности трудоустройства);

- офисные веб-приложения (SaaS-приложения, которые предоставляют услуги, аналогичные традиционным настольным офисным инструментам, включая текстовые редакторы, электронные таблицы и презентации. Примерами таких приложений являются Google Docs, Google Sheets, Microsoft 365, Zoho Docs, Dropbox Paper);

- стриминговые сервисы и телевидение (потоковая передача медиаконтента, в том числе трансляции радио и телевидения через интернет);

- торренты и сети peer-to-peer (сайты, агрегирующие ссылки BitTorrent для обмена файлами);

- сайты знакомств;

- сайты, содержащие порнографические материалы;

- веб-почта (сервисы электронной почты. Предоставляют доступ к почтовому ящику, позволяя пользователям отправлять и получать электронные письма, как правило, предлагая бесплатный или платный публичный доступ к таким услугам);

- спам (сайты, URL-адреса которых часто встречаются в спам-письмах или нежелательных коммерческих сообщениях);
- частные IP-адреса (IP-адреса, определенные в RFC 1918 — «Выделение адресов для частных интрасетей»);
- сайты рекламных и баннерных сетей (онлайн-реклама, медиа, баннеры и промоконтент).

4.4.7 Требования к инспекции зашифрованного трафика

4.4.7.1 Межсетевой экран нового поколения должен иметь возможность проксировать и инспектировать трафик протоколов TLS 1.2 и TLS 1.3.

4.4.7.2 Межсетевой экран нового поколения должен иметь возможность детектировать приложения прикладного уровня, сетевые атаки, вредоносный код, запрашиваемые URL в зашифрованном SSL/TLS-трафике.

4.4.7.3 Межсетевой экран нового поколения должен иметь возможность задания квалификаторов (как минимум IP-адресов источника и назначения, TCP/UDP-портов, пользователя или группы пользователей, URL-категории) для расшифровки SSL/TLS-трафика.

4.4.7.4 Межсетевой экран нового поколения должен иметь возможность задания квалификаторов (как минимум IP-адресов источника и назначения, TCP/UDP-портов, учетную запись пользователя или группы пользователей, URL-категории) для выборочного исключения SSL/TLS-трафика из расшифровки.

4.4.8 Требования к возможности организации отказоустойчивого кластера

4.4.8.1 Должна поддерживаться возможность кластеризации компонентов «Межсетевой экран» для обеспечения отказоустойчивости в режиме «активный — резервный» (active-standby).

4.4.8.2 Для межсетевых экранов, объединенных в отказоустойчивые кластеры (active-standby), должна обеспечиваться синхронизация конфигураций и сессий с верификацией работоспособности конфигурации на одном из межсетевых экранов, входящих в кластер.

4.4.8.3 Межсетевой экран нового поколения должен поддерживать возможность автоматического переключения на резервный межсетевой экран при сбоях выбранных сетевых интерфейсов.

4.4.8.4 Каждый из узлов отказоустойчивого кластера должен передавать в Модуль управления не только свои метрики здоровья, но и метрики здоровья соседа (в случае потери им связи с системой управления).

4.4.9 Требования к интеграции с внешними системами

4.4.9.1 ПАК «Межсетевой экран» должен поддерживать возможность управления через REST API.

4.4.9.2 Для организации удаленного управления через REST API должен быть использован защищенный протокол HTTPS на основе TLS и тип контента application/json.

4.4.9.3 Межсетевой экран нового поколения должен поддерживать возможность интеграции по протоколу ICAP (RFC 3507) с замкнутыми средами предварительного выполнения программ («песочницами» или «решениями класса sandbox»).

4.4.9.4 Должна поддерживаться возможность отправки информации о зарегистрированных событиях безопасности во внешние системы сбора и анализа событий по протоколу syslog.

4.4.10 Требования к организации защищенных каналов связи

4.4.10.1 Межсетевой экран нового поколения должен иметь возможность обеспечивать защиту (обеспечение конфиденциальности и целостности) информации, передаваемой по каналам связи.

4.4.10.2 Межсетевой экран нового поколения должен иметь возможность организации VPN-сети без изменения существующей физической инфраструктуры ЛВС.

4.4.10.3 Межсетевой экран нового поколения должен иметь поддержку возможности установления соединения на основе различных защищенных протоколов и стандартов (включая, но не ограничиваясь, IPSec).

4.4.10.4 Требуется поддержка как минимум следующих алгоритмов шифрования: AES-GCM-128/256, AES-CBC-128/256, 3DES, DES.

4.4.10.5 Требуется поддержка как минимум следующих алгоритмов для аутентификации: SHA-512/384/256, SHA-1, MD5.

4.4.10.6 Требуется поддержка как минимум следующих алгоритмов для обмена ключами: ECDH-384 (20), ECDH-256 (19), DH-3072 (15), DH-2048 (14), DH-1024(2), DH-768(1).

4.4.10.7 Требуется поддержка механизма, который гарантирует криптографическую защиту ранее переданных данных при компрометации долгосрочных ключей (Perfect Forward Secrecy (PFS).

4.4.11 Требования к функциям диагностики

4.4.11.1 ПАК «Межсетевой экран» и должен поддерживать возможность использования интерфейса командной строки для диагностирования сетевых проблем, просмотра и удаления установленных сессий.

4.4.12 Требования к Модулю управления

4.4.12.1 Модуль управления должен обеспечивать централизованное управление межсетевыми экранами через встроенный сетевой интерфейс взаимодействия с межсетевыми экранами.

4.4.12.2 В системе управления должен быть реализован ролевой метод управления доступом.

4.4.12.3 Ролевая модель межсетевого экрана нового поколения должна включать как минимум следующие роли:

- администратор безопасности;

- администратор межсетевого экрана;
- администратор информационной (автоматизированной) системы.

4.4.12.4Должна обеспечиваться возможность управления учетными записями пользователей межсетевого экрана нового поколения:

- идентификаторами (логинами) и паролями;
- назначенными ролями.

4.4.12.5Модуль управления должен поддерживать возможность формирования (создания) правил фильтрации сетевого трафика для определения разрешения или запрета (блокировки) прохождения сетевого трафика или сетевых пакетов на основе квалификаторов.

4.4.12.6Модуль управления должен поддерживать возможность включения, отключения, редактирования и удаления созданных правил фильтрации.

4.4.12.7Модуль управления должен предоставлять возможность объединения нескольких межсетевых экранов в группы устройств.

4.4.12.8Модуль управления должен предоставлять возможность создания иерархии групп устройств, в которой правила фильтрации сетевого трафика, созданные для родительской группы устройств, наследуются межсетевыми экранами всех дочерних групп устройств.

4.4.12.9Модуль управления должен предоставлять возможность создания объектов (адресов, групп адресов, портов TCP/UDP, групп портов) с привязкой объектов и групп объектов к различным уровням иерархии групп устройств межсетевого экранирования с тем, чтобы при создании политик безопасности отображались только объекты управления соответствующего уровня иерархии.

4.4.12.10 Модуль управления должен осуществлять регистрацию и журналирование успешных и неуспешных (в том числе заблокированных) сетевых соединений, включая (но не ограничиваясь):

- дату и время инициации соединения;
- идентификатор пользователя, инициировавшего соединение;
- сетевой протокол соединения, используемые TCP/UDP-порты;
- IP-адреса сетевых активов, с которых и на которые инициировано соединение;

- идентификатор приложения, взаимодействующего через межсетевой экран;
- обнаружение активности вредоносного ПО;
- зафиксированные сетевые атаки на защищаемые сетевые активы.

4.4.12.11 Модуль управления должен предоставлять возможности просмотра всех событий безопасности в журнале событий безопасности межсетевого экрана и выборочного просмотра событий безопасности (фильтрация событий безопасности).

4.4.12.12 Модуль управления должен предоставлять возможность поиска необходимых записей в журналах, политик и объектов не только по названию, но и по содержимому политик и объектов.

4.4.12.13 Модуль управления должен предоставлять возможность создания резервной копии всех настроек системы управления, скачивания резервной копии и восстановления из созданной ранее резервной копии.

4.5 Требования назначения

4.5.1 Общие требования

4.5.1.1 Межсетевой экран нового поколения должен обеспечивать высокую пропускную способность сетевого трафика с минимальной задержкой с тестированием по профилю EMIX, указывающему соотношение объема передаваемого трафика в секунду через межсетевой экран.

Таблица 1 — Распределение трафика приложений в профиле Application Mix

Тип трафика	Процент от общей пропускной способности, %	Тип трафика	Процент от общей пропускной способности, %
TLS	72,86	syslog	0,87
HTTP[1]	6,84	POP3	0,78

[1] HTTP-трафик, проходящий через межсетевой экран в любом направлении, с размером полезной нагрузки потока до 64 КБ.

SMB	5,93	SSH	0,67
RDP	4,74	IMAP	0,59
NFS	3,75	DNS	0,32
SIP	1,37	Неизвестно	0,04
SMTP	1,24		

4.5.2 Требования к производительности и поддерживаемым функциям межсетевого экрана нового поколения

4.5.2.1 ПАК «Межсетевой экран» должен обеспечивать следующие показатели функциональности и производительности:

Таблица 2 — Характеристики межсетевого экрана тип 1

№	Характеристика	Значение
1	Пропускная способность в режиме межсетевого экранирования с инспекцией состояния (stateful firewall) с настроенными правилами фильтрации (не менее 10 000 правил), на профиле трафика EMIX	Не менее 8 Гбит/с
2	Пропускная способность с обеспечением идентификации приложений и пользователей с включенными функциями системы предотвращения вторжений (IPS), на профиле трафика EMIX	Не менее 1,4 Гбит/с

№	Характеристика	Значение
3	Пропускная способность с обеспечением идентификации приложений и пользователей с включенными функциями проверки трафика приложений на наличие признаков угроз сетевых атак (IPS, антивирус), а также активированным модулем URL-фильтрации, на профиле трафика EMIX	Не менее 1 Гбит/с
4	Инспекция TLS/SSL в режиме TLS Forward Proxy	Не менее 800 Мбит/с
5	Производительность	Не менее 1,1 млн. пакетов/секунду
6	Число поддерживаемых правил фильтрации	Не менее 10 000
7	Количество одновременных L7-сессий (HTTP- трафик), 1КБ	Не менее 1,3 млн.
8	Количество новых сессий в секунду (HTTP-транзакции размером 1 байт)	Не менее 80 тыс. сессий/секунду
9	Число поддерживаемых VLAN	Не менее 4094
10	Число поддерживаемых зон безопасности	Не менее 65535
11	Трансляция сетевых адресов (NAT)	source NAT, destination NAT
12	Поддержка каталогов LDAP	Microsoft Active Directory
13	Встроенная подсистема распознавания приложений	Наличие
14	Агрегация каналов	Статический LAG, LACP

№	Характеристика	Значение
15	Поддержка протоколов маршрутизации	Статическая маршрутизация, OSPF, BGP
16	Поддержка BGP Community list	Наличие
17	Поддержка функции BFD (Bidirectional Forwarding Detection)	Multi-hop BFD (RFC 5883), BFD для OSPF/BGP, BFD для статических маршрутов
18	Поддержка Policy-based Routing (PBR)	Наличие
19	Поддержка Graceful restart для OSPF (RFC 3623)	Наличие
20	Поддержка Graceful restart для BGP (RFC 4724, RFC 8538)	Наличие
21	Поддержка SNMP v2c, v3	Наличие
22	Поддержка DHCP-Relay	Наличие
23	Поддержка виртуальных контекстов безопасности	Наличие
24	Количество поддерживаемых виртуальных контекстов	Не менее 256
25	Количество поддерживаемых виртуальных таблиц маршрутизации (VRF) в рамках уникального контекста	Не менее 256
26	Зеркалирование дешифрованного трафика на сторонние системы	Наличие
27	Отправка сообщений журналов на сторонние системы по протоколу syslog	Наличие

№	Характеристика	Значение
28	Возможность редактирования таймаутов сессий (как TCP, так и UDP) глобально на межсетевом экране, на уровне виртуального контекста и для отдельного сервиса	Наличие
29	Возможность создания собственных сервисов на основе номера IP протокола	Наличие
30	Режимы работы сетевых интерфейсов межсетевого экрана	Маршрутизация (L3) Виртуальное соединение (vWire)
31	Возможность одновременной работы различных субинтерфейсов одного физического порта в режимах маршрутизации и виртуального соединения	Наличие

Таблица 3 — Характеристики межсетевого экрана тип 2

№	Характеристика	Значение
1	Пропускная способность в режиме межсетевого экранирования с инспекцией состояния (stateful firewall) с настроенными правилами фильтрации (не менее 100 000 правил), на профиле трафика EMIX	Не менее 80 Гбит/с
2	Пропускная способность с обеспечением идентификации приложений и пользователей с включенными функциями системы предотвращения вторжений (IPS), на профиле трафика EMIX	Не менее 12 Гбит/с

№	Характеристика	Значение
3	Пропускная способность с обеспечением идентификации приложений и пользователей с включенными функциями проверки трафика приложений на наличие признаков угроз сетевых атак (IPS, антивирус), а также активированным модулем URL-фильтрации, на профиле трафика EMIX	Не менее 10 Гбит/с
4	Инспекция TLS/SSL в режиме TLS Forward Proxy	Не менее 8 Гбит/с
5	Производительность	Не менее 7 млн. пакетов/секунду
6	Число поддерживаемых правил фильтрации	Не менее 100 000
7	Количество одновременных L7-сессий (HTTP-трафик)	Не менее 6,4 млн.
8	Количество новых сессий в секунду (HTTP-транзакции размером 1 байт)	Не менее 900 тыс. сессий/секунду
9	Число поддерживаемых VLAN	4094
10	Число поддерживаемых зон безопасности	Не менее 65535
11	Трансляция сетевых адресов (NAT)	source NAT, destination NAT
12	Поддержка каталогов LDAP	Microsoft Active Directory
13	Встроенная подсистема распознавания приложений	Наличие
14	Агрегация каналов	Статический LAG, LACP

№	Характеристика	Значение
15	Поддержка протоколов маршрутизации	Статическая маршрутизация, OSPF, BGP
16	Поддержка BGP Community list	Наличие
17	Поддержка функции BFD (Bidirectional Forwarding Detection)	Multi-hop BFD (RFC 5883), BFD для OSPF/BGP, BFD для статических маршрутов
18	Поддержка Policy-based Routing (PBR)	Наличие
19	Поддержка Graceful restart для OSPF (RFC 3623)	Наличие
20	Поддержка Graceful restart для BGP (RFC 4724, RFC 8538)	Наличие
21	Поддержка SNMP v2c, v3	Наличие
22	Поддержка DHCP-Relay	Наличие
23	Поддержка виртуальных контекстов безопасности	Наличие
24	Количество поддерживаемых виртуальных контекстов	Не менее 256
25	Количество поддерживаемых виртуальных таблиц маршрутизации (VRF) в рамках уникального контекста	Не менее 256
26	Зеркалирование дешифрованного трафика на сторонние системы	Наличие
27	Отправка сообщений журналов на сторонние системы по протоколу syslog	Наличие

№	Характеристика	Значение
28	Возможность редактирования таймаутов сессий (как TCP, так и UDP) глобально на межсетевом экране, на уровне виртуального контекста и для отдельного сервиса	Наличие
29	Возможность создания собственных сервисов на основе номера IP протокола	Наличие
30	Режимы работы сетевых интерфейсов межсетевого экрана	Маршрутизация (L3) Виртуальное соединение (vWire)
31	Возможность одновременной работы различных субинтерфейсов одного физического порта в режимах маршрутизации и виртуального соединения	Наличие

4.5.3 Требования к функциональности и масштабируемости модуля управления

4.5.3.1 Модуль управления должен обеспечивать выполнение функций по настройке и управлению всех ПАК «Межсетевой экран», описанных в данном документе.

4.5.3.2 Модуль управления должен обеспечивать показатели функциональности и масштабируемости.

4.6 Требования к документации

4.6.1 Общие требования к документации

4.6.1.1 Поставляемые межсетевые экраны нового поколения должны иметь эксплуатационную документацию на русском языке, поставляемую в бумажном или электронном виде совместно с товаром, или доступную на сайте производителя межсетевых экранов нового поколения.

4.7 Требования к технической поддержке

4.7.1 Общие требования к технической поддержке

4.7.1.1 Производитель межсетевого экрана нового поколения должен обеспечить техническую поддержку в режиме 24/7 (круглосуточно, ежедневно). Техническая поддержка должна включать в себя следующий набор услуг:

- предоставление доступа к обновленным версиям продукта;
- помощь в восстановлении работоспособности продукта в случае программного сбоя или неправильных настроек;
- консультации по работе и настройке продукта;
- устранение ошибок и дефектов в работе продукта в рамках выпуска обновлений;
- рассмотрение предложений по доработке продукта;
- круглосуточный доступ к порталу техобслуживания поставщика межсетевых экранов нового поколения для создания и обновления заявок, а также для чтения новостей о продукте;
- авансовая замена оборудования в случае аппаратных неисправностей с отгрузкой со склада не позднее чем на следующий календарный день;

4.7.1.2 Длительность оказания технической поддержки должна составлять не менее 12 (двеннадцати) месяцев с даты поставки.

Таблица 4 — Характеристики ПАК «Межсетевой экран» тип 1.

№	Характеристика	Значение
1	Число процессоров	Не менее 1 шт.
2	Тип процессора	Intel Atom или эквивалент
3	Число ядер одного процессора	Не менее 8
4	Тактовая частота процессора	Не ниже 2,20 ГГц
5	ОЗУ	Не менее 32 ГБ
6	Тип ОЗУ	DDR не ранее 4-го поколения
7	Тип и число дисков	Не менее 1 шт., тип SSD NVME
8	Объем твердотельного накопителя	Не менее 240 ГБ
9	Консольный порт	Не менее 1 шт., RJ-45
10	Порты USB	Не менее 2 шт.
11	Сетевые интерфейсы	Не менее 4 портов с поддержкой скоростей не ниже 1 Гбит/с, RJ-45 медный. Не менее 4 портов с поддержкой скоростей не ниже 10 Гбит/с, SFP+.
12	Трансиверы	В комплекте поставки с каждым ПАК «Межсетевой экран» должны быть включены следующие трансиверы: - 2 шт. трансивер форм-фактора SFP+, 10 Гбит/с, 300 м, 850nm, LC, DDM.

№	Характеристика	Значение
		Совместимость трансиверов с поставляемым оборудованием должна быть подтверждена производителем ПАК «Межсетевой экран».
13	Число блоков питания	Не менее 2 шт.
14	Мощность блоков питания	Не более 60 Вт
15	Форм-фактор	Настольный, с возможностью монтажа в стойку 19’, не более 1RU
6	Габаритные размеры (Г х Ш х В)	Не более 185 х 300 х 44 мм

Таблица5 — Характеристики ПАК «Межсетевой экран» тип 2.

№	Характеристика	Значение
1	Число процессоров	Не менее 1 шт.
2	Число ядер одного процессора	Не менее 16
3	Тип процессора	Intel Xeon Scalable не ранее 4-го поколения или эквивалент
4	ОЗУ	Не менее 128 ГБ
5	Тип ОЗУ	DDR не ранее 5-го поколения
6	Тип и число дисков	Не менее 2 шт., тип SSD NVMe
7	Объем твердотельного накопителя	Не менее 240 ГБ
8	Выделенный порт управления	Не менее 1 шт., RJ-45, со скоростью не ниже 1 Гбит/с

№	Характеристика	Значение
9	Консольный порт	Не менее 1 шт., RJ-45
10	Порты USB	Не менее 2 шт.
11	Сетевые интерфейсы	Не менее 4 портов с поддержкой скоростей не ниже 1 Гбит/с, SFP, RJ-45 медный. Не менее 2 портов с поддержкой скоростей не ниже 10/25 Гбит/с, SFP28.
12	Трансиверы	В комплекте поставки с каждым ПАК «Межсетевой экран» должны быть включены следующие трансиверы: - 2 шт. трансивер форм-фактора SFP28, 25 Гбит/с, 100 м, Tx850nm, MM, LC, DDM; Совместимость трансиверов с поставляемым оборудованием должна быть подтверждена производителем ПАК «Межсетевой экран».
13	Возможность поддержки дополнительных сетевых интерфейсов	Аппаратная платформа должна предусматривать расширение портовой емкости картами: - 4 x 1 Гбит/с, RJ-45; - 2 x 10/25 Гбит/с, SFP28; - 4 x 10/25 Гбит/с, SFP28; - 2 x 100 Гбит/с, QSFP28.
14	Количество свободных слотов для карт расширения	Не менее 3
15	Число блоков питания	Не менее 2 шт.

№	Характеристика	Значение
16	Мощность блоков питания	Не более 1600 Вт
17	Форм-фактор	Для монтажа в стойку 19’, не более 2RU
18	Габаритные размеры (Г х Ш х В)	Не более 550 х 490 х 89 мм

Таблица 6 — Характеристики виртуальной машины «Модуль управления» тип 1.

№	Характеристика	Значение
1	Исполнение модуля управления	Образ виртуальной машины
2	Число поддерживаемых ПАК «Межсетевой экран»	Не менее 20 шт.
3	Поддержка систем виртуализации	ESXi не ниже версии 7, KVM

5. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К КОММУТАТОРАМ

5.1 Коммутатор уровня агрегации, L3, 48×1GbE + 2×40G + 4×25G

Количество: 2 шт.

№	Характеристика	Значение
1	Форм-фактор	1U, монтаж в 19" стойку
2	Габаритные размеры	442 × 430 × 43,6 мм

3	Уровень коммутации	L3 (поддержка маршрутизации)
4	Порты доступа (медь)	48 × 10/100/1000 Мбит/с (RJ-45)
5	Аплинки 40G	2 × 40 Гбит/с QSFP
6	Аплинки 25G	4 × 25 Гбит/с SFP28
7	Порты управления	1 × консольный RJ-45; 1 × управление Ethernet (RJ-45)
8	Стекирование	Физическое стекирование: до 9 коммутаторов, единый control-plane
9	Пропускная способность	600 Гбит/с
10	Таблица MAC-адресов	98 304 записей
11	Блоки питания	2 × модульных БП с горячей заменой; питание 100–240 В, 50–60 Гц; макс. потребляемая мощность 120 Вт
12	Вентиляторы	Модульные, с горячей заменой, интеллектуальная регулировка скорости
13	Поддержка VLAN	IEEE 802.1Q, QinQ (двойное тегирование)
14	Протоколы L2	STP/RSTP/MSTP, ERPS, G.8031, G.8032, MLAG, LACP, EFM (802.3ah), CFM (802.1ag), UDLD
15	Протоколы L3 (маршрутизация)	Static Routing, RIP, OSPF, IS-IS, BGP, uRPF, VRF, PBR, ECMP, VRRP, BFD
16	Туннелирование и оверлей	VxLAN, GRE, NVGRE, MPLS, IPv6 over IPv4, 6to4, ISATAP

17	Multicast	PIM-SM, PIM-SSM, PIM-DM, IGMP v1/v2/v3 (L3), MVR, IPMC
18	Безопасность	802.1X, AAA, RADIUS, TACACS+, Dot1x, Control Plane Policy (COPP), CPU Traffic Limit, защита от DDOS (ICMP Flood/Smurf/Fraggle/LAND/SYN Flood)
19	Мониторинг и управление	CLI, Web-интерфейс, SNMP v2c/v3, IPSLA, IPFIX, RPC-API, OVSDB, ERSPAN, Port Mirroring, Multi-destination mirror (m:n)
20	Сервисы DHCP	DHCP Server, Client, Relay, Snooping, Option 82, Option 252
21	QoS	WRED (Weighted Random Early Detection), port speed limit
22	Диагностика	VCT (Virtual Cable Test), port energy saving
23	Применение	Коммутатор уровня агрегации корпоративных / кампусных сетей

5.2 Коммутатор ядра, L3, 8×1GbE + 8×1G SFP + 12×10G SFP+ + 8×25G SFP28 + 2×40G QSFP

Количество: 2 шт.

№	Характеристика	Значение
1	Форм-фактор	1U, монтаж в 19" стойку
2	Уровень коммутации	L3 (поддержка маршрутизации)

3	Порты доступа (медь) 1G	8 × 10/100/1000 Мбит/с (RJ-45)
4	Порты SFP 1G	8 × 1 Гбит/с SFP
5	Порты SFP+ 10G	12 × 10 Гбит/с SFP+
6	Аплинки 40G	2 × 40 Гбит/с QSFP
7	Аплинки 25G	8 × 25 Гбит/с SFP28
8	Порты управления	1 × консольный RJ-45; 1 × управление Ethernet (RJ-45); 1 × USB
9	Стекирование	Физическое стекирование: до 9 коммутаторов, единый control-plane
10	Пропускная способность	800 Гбит/с
11	Таблица MAC-адресов	98 304 записей
12	Блоки питания	2 × модульных БП с горячей заменой; питание 100–240 В, 50–60 Гц; макс. потребляемая мощность 350 Вт
13	Вентиляторы	Модульные, с горячей заменой, интеллектуальная регулировка скорости
14	Поддержка VLAN	IEEE 802.1Q, QinQ (двойное тегирование)
15	Протоколы L2	STP/RSTP/MSTP, ERPS, G.8031, G.8032, MLAG, LACP, EFM (802.3ah), CFM (802.1ag), UDLD, VARP (Virtual-ARP)
16	Протоколы L3 (маршрутизация)	Static Routing, RIP, OSPF, IS-IS, BGP, uRPF, VRF, PBR, ECMP, VRRP, BFD

17	Туннелирование и оверлей	VxLAN, GRE, NVGRE, MPLS, IPv6 over IPv4, 6to4, ISATAP
18	Multicast	PIM-SM, PIM-SSM, PIM-DM, IGMP v1/v2/v3 (L3), MVR, IPMC
19	Безопасность	802.1X, AAA, RADIUS, TACACS+, Dot1x, Control Plane Policy (COPP), CPU Traffic Limit, защита от DDOS (ICMP Flood/Smurf/Fraggle/LAND/SYN Flood)
20	Мониторинг и управление	CLI, Web-интерфейс, SNMP v2c/v3, IPSLA, IPFIX, RPC-API, OVSDB, ERSPAN, Port Mirroring, Multi-destination mirror (m:n)
21	Сервисы DHCP	DHCP Server, Client, Relay, Snooping, Option 82, Option 252
22	QoS	WRED (Weighted Random Early Detection), port speed limit
23	Диагностика	VCT (Virtual Cable Test), port energy saving
24	Применение	Коммутатор ядра корпоративных / кампусных сетей, MAN, гиперконвергентная инфраструктура

5.3 Коммутатор доступа, L3, 24×1GbE + 2×40G + 4×25G
Количество: 3 шт.

№	Характеристика	Значение
1	Форм-фактор	1U, монтаж в 19" стойку
2	Уровень коммутации	L3 (поддержка маршрутизации)

3	Порты доступа (медь)	24 × 10/100/1000 Мбит/с (RJ-45)
4	Аплинки 40G	2 × 40 Гбит/с QSFP
5	Аплинки 25G	4 × 25 Гбит/с SFP28
6	Порты управления	1 × консольный RJ-45; 1 × управление Ethernet (RJ-45)
7	Стекирование	Физическое стекирование: до 9 коммутаторов, единый control-plane
8	Пропускная способность	128 Гбит/с
9	Таблица MAC-адресов	98 304 записей
10	Блоки питания	2 × модульных БП с горячей заменой; питание 100–240 В, 50–60 Гц; макс. потребляемая мощность 120 Вт
11	Вентиляторы	Модульные, с горячей заменой, интеллектуальная регулировка скорости
12	Поддержка VLAN	IEEE 802.1Q, QinQ (двойное тегирование)
13	Протоколы L2	STP/RSTP/MSTP, ERPS, G.8031, G.8032, MLAG, LACP, EFM (802.3ah), CFM (802.1ag), UDLD
14	Протоколы L3 (маршрутизация)	Static Routing, RIP, OSPF, IS-IS, BGP, uRPF, VRF, PBR, ECMP, VRRP, BFD
15	Туннелирование и оверлей	VxLAN, GRE, NVGRE, MPLS, IPv6 over IPv4, 6to4, ISATAP

16	Multicast	PIM-SM, PIM-SSM, PIM-DM, IGMP v1/v2/v3 (L3), MVR, IPMC
17	Безопасность	802.1X, AAA, RADIUS, TACACS+, Dot1x, Control Plane Policy (COPP), CPU Traffic Limit
18	Мониторинг и управление	CLI, Web-интерфейс, SNMP v2c/v3, IPSLA, IPFIX, RPC-API, OVSDB, ERSPAN, Port Mirroring
19	Сервисы DHCP	DHCP Server, Client, Relay, Snooping, Option 82, Option 252
20	QoS	WRED (Weighted Random Early Detection), port speed limit
21	Применение	Коммутатор уровня доступа корпоративных / кампусных сетей

5.4 Коммутатор доступа, L3, 48×1GbE + 2×40G + 4×25G
Количество: 4 шт.

№	Характеристика	Значение
1	Форм-фактор	1U, монтаж в 19" стойку
2	Габаритные размеры	442 × 430 × 43,6 мм
3	Уровень коммутации	L3 (поддержка маршрутизации)
4	Порты доступа (медь)	48 × 10/100/1000 Мбит/с (RJ-45)
5	Аплинки 40G	2 × 40 Гбит/с QSFP
6	Аплинки 25G	4 × 25 Гбит/с SFP28

7	Порты управления	1 × консольный RJ-45; 1 × управление Ethernet (RJ-45)
8	Стекирование	Физическое стекирование: до 9 коммутаторов, единый control-plane
9	Пропускная способность	600 Гбит/с
10	Таблица MAC-адресов	98 304 записей
11	Блоки питания	2 × модульных БП с горячей заменой; питание 100–240 В, 50–60 Гц; макс. потребляемая мощность 120 Вт
12	Вентиляторы	Модульные, с горячей заменой, интеллектуальная регулировка скорости
13	Поддержка VLAN	IEEE 802.1Q, QinQ (двойное тегирование)
14	Протоколы L2	STP/RSTP/MSTP, ERPS, G.8031, G.8032, MLAG, LACP, EFM (802.3ah), CFM (802.1ag), UDLD
15	Протоколы L3 (маршрутизация)	Static Routing, RIP, OSPF, IS-IS, BGP, uRPF, VRF, PBR, ECMP, VRRP, BFD
16	Туннелирование и оверлей	VxLAN, GRE, NVGRE, MPLS, IPv6 over IPv4, 6to4, ISATAP
17	Multicast	PIM-SM, PIM-SSM, PIM-DM, IGMP v1/v2/v3 (L3), MVR, IPMC
18	Безопасность	802.1X, AAA, RADIUS, TACACS+, Dot1x, Control Plane Policy (COPP), CPU Traffic Limit, защита от DDOS (ICMP Flood/Smurf/Fraggle/LAND/SYN Flood)

19	Мониторинг и управление	CLI, Web-интерфейс, SNMP v2c/v3, IPSLA, IPFIX, RPC-API, OVSDB, ERSPAN, Port Mirroring, Multi-destination mirror (m:n)
20	Сервисы DHCP	DHCP Server, Client, Relay, Snooping, Option 82, Option 252
21	QoS	WRED (Weighted Random Early Detection), port speed limit
22	Диагностика	VCT (Virtual Cable Test), port energy saving
23	Применение	Коммутатор уровня агрегации корпоративных / кампусных сетей

5.5 Коммутатор доступа, L2+, 8*10/100/1000Base-T PoE 802.3af/at + 2*1000/2500Base-X SFP, дальность до 250м, 120Вт
Количество: 5 шт.

5.6 Коммутатор доступа, L2/L3, 24×1GbE + 4×10G SFP+
Количество: 24 шт.

№	Характеристика	Значение
1	Форм-фактор	1U, монтаж в 19" стойку
2	Уровень коммутации	L2/L3 (базовая маршрутизация)
3	Порты доступа (медь)	24 × 10/100/1000 Мбит/с (RJ-45)
4	Аплинки 10G	4 × 10 Гбит/с SFP+

5	Порты управления	1 × консольный RJ-45; 1 × USB-серийный порт
6	Пропускная способность	128 Гбит/с
7	Буфер пакетов	95,23 Mpps
8	Таблица MAC-адресов	16 000 записей
9	Блок питания	1 × БП; питание 100–240 В, 50–60 Гц; макс. потребляемая мощность 36 Вт
10	Поддержка VLAN	IEEE 802.1Q (тегирование VLAN), QinQ
11	Протоколы L2	STP/RSTP/MSTP, LACP (агрегация портов / LAG), 802.1X, Port Mirroring
12	Протоколы L3 (маршрутизация)	Static Routing, RIP, OSPF stub
13	Multicast	IGMP v1/v2/v3 (L3)
14	Безопасность	AAA, RADIUS, TACACS+, 802.1X, защита от DoS атак (автоматическая), CPU protection policy
15	QoS	Port speed limit, QoS политики
16	Мониторинг и управление	CLI, Web-интерфейс, SNMP v2c/v3, Port Mirroring, port energy saving
17	Применение	Коммутатор уровня доступа на объектах

6. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К СЕРВЕРУ И ВСПОМОГАТЕЛЬНОМУ ОБОРУДОВАНИЮ

6.1 Сервер управления и приложений

Количество: 1 шт.

Поставляемый сервер должен быть предназначен для размещения в стойке и использования в составе корпоративной информационной инфраструктуры, включая, но не ограничиваясь, задачами виртуализации, размещения прикладных систем, сервисов каталогов, баз данных, сетевых сервисов, терминальных служб, резервного копирования и иных вычислительных нагрузок.

Сервер должен обеспечивать круглосуточную эксплуатацию в центре обработки данных или серверной комнате, поддерживать удаленное администрирование, резервирование критичных узлов и возможность дальнейшего масштабирования конфигурации.

6.1.1 Конструктивное исполнение

Тип оборудования: сервер стоечный.

Форм-фактор: не более 1U.

Исполнение: для установки в стандартную 19-дюймовую телекоммуникационную или серверную стойку.

Направляющие и крепеж для монтажа в стойку должны входить в комплект поставки.

Все основные заменяемые узлы должны быть выполнены в промышленном исполнении, пригодном для эксплуатации в серверной среде.

6.1.2 Процессорная подсистема

Сервер должен поддерживать установку до 2 процессоров серверного класса Intel Xeon Scalable соответствующей платформы.

Поставляемая конфигурация должна включать не менее 2 установленных процессоров.

Каждый установленный процессор должен иметь не менее 16 физических ядер.

Базовая тактовая частота каждого установленного процессора должна быть не менее 2.0 ГГц.

Поддержка технологий многопоточности, аппаратной виртуализации и расширенных инструкций для серверных вычислений обязательна.

Предлагаемая конфигурация должна обеспечивать штатную работу всех установленных модулей памяти, контроллеров ввода-вывода и дисковой подсистемы без ограничений по совместимости.

6.1.3 Оперативная память

Сервер должен иметь не менее 32 слотов под модули оперативной памяти типа RDIMM DDR5.

Платформа должна поддерживать суммарный объем оперативной памяти до 8 ТБ.

Поддерживаемая скорость памяти должна составлять до 4800 MT/s или выше при наличии соответствующей поддержки платформы.

Поставляемая конфигурация должна быть укомплектована оперативной памятью объемом не менее 256 ГБ.

Оперативная память должна быть установлена симметрично по каналам, в соответствии с рекомендациями производителя.

Все модули памяти должны быть одного типа и совместимы с установленными процессорами и системной платой.

6.1.4 Подсистема хранения данных

Сервер должен поддерживать установку фронтальных накопителей форм-фактора 2.5 дюйма с интерфейсами SAS, SATA и/или NVMe в зависимости от конфигурации.

Сервер должен поддерживать установку не менее 8 фронтальных накопителей 2.5 дюйма; предпочтительно — до 10 накопителей 2.5 дюйма.

Допускается наличие дополнительных задних отсеков для накопителей 2.5 дюйма как опция или в составе поставки.

Поставляемая конфигурация должна включать дисковую подсистему общим полезным объемом не менее 7.68 ТБ.

Накопители должны быть серверного класса, предназначенными для круглосуточной эксплуатации.

Для системного раздела допускается использование выделенных загрузочных устройств или отдельного RAID-массива.

6.1.5 RAID и контроллеры хранения

Сервер должен поддерживать аппаратные RAID-контроллеры семейства PERC либо эквивалентные решения серверного класса.

Должна быть обеспечена поддержка уровней RAID не ниже 1, 5, 10.
Контроллер хранения должен иметь кэш-память или функциональный эквивалент, предусмотренный производителем платформы.
Поставляемая конфигурация должна включать установленный и настроенный RAID-контроллер, совместимый с выбранной подсистемой хранения.
При использовании загрузочных модулей BOSS или аналогичных решений они должны быть полностью совместимы с платформой сервера.

6.1.6 Сетевые интерфейсы

Сервер должен иметь не менее 2 сетевых портов Ethernet.
Скорость сетевых интерфейсов должна составлять не менее 10 Гбит/с на каждый порт; допускается предложение портов 1/10/25 Гбит/с или выше в зависимости от конфигурации и применяемой сетевой карты.
Платформа должна поддерживать сетевые адаптеры формата OCP 3.0 или эквивалентного серверного стандарта.
Должен быть предусмотрен выделенный интерфейс удаленного управления.
Сетевые адаптеры и трансиверы, если они необходимы для ввода оборудования в эксплуатацию, должны быть совместимы между собой и с поставляемым сервером.

6.1.7 Слоты расширения и ввод-вывод

Сервер должен поддерживать не менее 2 слотов расширения PCI Express; предпочтительно — до 3 слотов в зависимости от райзера и конфигурации.
Конфигурация должна допускать установку дополнительных сетевых адаптеров, контроллеров хранения и иных карт расширения в рамках ограничений платформы.
Должны быть предусмотрены стандартные сервисные порты для локального обслуживания, включая USB и видеовыход, если они предусмотрены штатной платформой.

6.1.8 Удаленное управление и мониторинг

Сервер должен быть оснащен встроенным контроллером удаленного управления уровня iDRAC9 либо функционально эквивалентным решением.

Удаленное управление должно обеспечивать:
включение, выключение и перезагрузку сервера;
просмотр аппаратного состояния и журналов событий;
удаленную консоль;
удаленное подключение образов для установки операционной системы;
мониторинг состояния процессоров, памяти, вентиляторов, дисков и блоков питания.
Средства управления должны поддерживать работу через веб-интерфейс и сетевой доступ администратора.

6.1.9 Подсистема питания и охлаждения

Сервер должен поддерживать установку двух резервируемых блоков питания с возможностью горячей замены.
Поставляемая конфигурация должна включать 2 блока питания.
Мощность каждого блока питания должна быть достаточной для штатной работы поставляемой конфигурации с учетом резервирования по схеме N+1.
Платформа должна поддерживать варианты блоков питания различной мощности, включая серверные AC/DC-модули в зависимости от конфигурации.
Система охлаждения должна быть штатной, серверного исполнения, с автоматическим регулированием производительности вентиляторов.

6.1.10 Совместимость с ПО

Сервер должен поддерживать установку современных серверных операционных систем и гипервизоров, предусмотренных производителем платформы.
Оборудование должно быть пригодно для эксплуатации в средах виртуализации и многопользовательских вычислительных нагрузках.
Драйверы, микропрограммы и утилиты управления должны быть доступны на официальном сайте производителя.

№	Характеристика	Значение
1	Форм-фактор	Стоечный, не более 1U

2	Процессоры	2 × Intel Xeon Gold 6526Y (6-го поколения или новее)
3	ОЗУ	Не менее 256 ГБ DDR5
4	Накопители	Не менее 5 × 3,84 ТБ SSD (конфигурируются в RAID 10)
5	Интерфейс управления	IPMI/iDRAC или аналог
6	Сетевой интерфейс	Не менее 2 сетевых портов Ethernet. Скорость сетевых интерфейсов должна составлять не менее 10 Гбит/с на каждый порт и необходимые кабели для подключения в сетевую инфраструктуру.
7	Гарантия	Не менее 1 года

6.2 Кабель DAC SFP+ 2 м

Количество: 15 шт.

№	Характеристика	Значение
1	Тип	Direct Attach Copper (DAC)
2	Форм-фактор	SFP+
3	Длина	2 м
4	Скорость	10 Гбит/с

6.3 Шкаф телекоммуникационный настенный 12U в сборе

Количество: 24 компл.

Каждый шкаф должен поставляться в сборе и включать:

№	Наименование компонента	Кол-во

1	Шкаф настенный 12U, Ш=600 мм, Г=650 мм, RAL 9005	1 шт.
2	Патч-панель 19", 24 порта, STP	2 шт.
3	Кабельный органайзер 19", 1U	1 шт.
4	Комплект заземления + панель заземления	1 компл.
5	Монтажный комплект	1 шт.
6	Блок силовых розеток 19", 9 розеток	1 шт.
7	Полка перфорированная 19"	2 шт.

6.4 Активный Кабель DAC QSFP 1 м

Количество: 4 шт.

№	Характеристика	Значение
1	Тип	Активный оптический (AOC) на базе многомодового волокна OM3/OM4
2	Форм-фактор	QSFP
3	Длина	1 м
4	Скорость	40 Гбит/с

7. ТРЕБОВАНИЯ К ВЫПОЛНЯЕМЫМ РАБОТАМ

7.1 Перечень работ

Исполнитель обязан выполнить следующие виды работ:

№	Наименование работы	Кол-во
1	Установка и настройка коммутаторов агрегации	1 шт.

2	Установка и настройка NGFW тип 1 (кластер Active/Passive)	1 шт.
3	Установка и настройка СКЗИ тип 1	1 шт.
4	Установка и настройка сервера	1 шт.
5	Установка и настройка коммутаторов ядра и доступа	1 шт.
6	Установка и настройка NGFW тип 2 (кластер Active/Passive)	1 шт.
7	Установка и настройка СКЗИ тип 2	1 шт.
8	Установка и настройка коммутаторов	1 шт.
9	Установка и настройка СКЗИ тип 2	1 шт.
10	Сборка и установка телекоммуникационных шкафов (24 объекта)	1 шт.

7.2 Требования к составу работ

В рамках каждого вида работ исполнитель должен выполнить:

- физический монтаж оборудования в стойку/шкаф или на поверхность;
- подключение кабельной инфраструктуры (коммутационные кабели, трансиверы, DAC);
- первоначальную настройку согласно проектной документации: IP-адресация, маршрутизация, VLAN, политики безопасности, VPN-туннели, кластеризация NGFW;
- тестирование работоспособности: проверку прохождения трафика через VPN-туннели, работы кластеров Active/Passive, доступности ресурсов;
- сдачу результатов Заказчику с оформлением акта выполненных работ.

7.3 Требования к документации по результатам работ

Исполнитель обязан передать Заказчику:

- исполнительную документацию с фактической конфигурацией оборудования;
- схему IP-адресации и таблицу маршрутизации;
- перечень созданных VPN-туннелей и политик безопасности;
- акт приёмки выполненных работ.

8. ТРЕБОВАНИЯ К ГАРАНТИИ

Позиция	Гарантийный срок
ПАК СКЗИ тип 1 и тип 2	Не менее 12 месяцев
NGFW тип 1 и тип 2	Не менее 12 месяцев;
Коммутаторы	Не менее 12 месяцев
Сервер	Не менее 12 месяцев
Шкафы и комплектующие	Не менее 12 месяцев

9. ТРЕБОВАНИЯ К КОНФИДЕНЦИАЛЬНОСТИ

Все сведения о конфигурации сети, IP-адресации, политиках безопасности и иные технические параметры, ставшие известными Исполнителю в ходе выполнения работ, являются конфиденциальными и не подлежат раскрытию третьим лицам.

Начальник ОИТиПТО **А.П. Курлович**