

Цели

Основной целью модернизации существующей сети передачи данных АО «УзРТСБ» является обеспечения бесперебойной работы электронных систем, а именно:

- Обеспечение отказоустойчивости компонентов сетевой инфраструктуры;
- Обеспечение безопасности границы сети и защиты от вторжений;
- Обеспечение безопасного доступа к ресурсам сети;
- Интеграция существующих вычислительных ресурсов ЦОД и устройств локальной вычислительной сети (ЛВС);
 - Увеличение скорости обработки сетевого трафика;
 - Сокращение времени простоя в случае сбоев;
 - Обеспечение возможности дальнейшего масштабирования и наращивания производительности информационной инфраструктуры АО «УзРТСБ».

Задачи

Для реализации цели модернизации существующей инфраструктуры сети передачи данных (сети) АО «УзРТСБ» должны быть выполнены следующие задачи:

- Создание отказоустойчивой системы безопасности границы сети путем приобретения программно-аппаратного комплекса межсетевых экранов;
- Создание отказоустойчивого ядра сети путем приобретения высокопроизводительных коммутаторов;
- Создание отказоустойчивой системы коммутации сети центра обработки данных (ЦОД) путем приобретения высокопроизводительных коммутаторов;
- Создание инфраструктуры системы управления сетевыми компонентами;
- Дооснащение существующей сети путём приобретения современных коммутаторов уровня доступа.

1. Технические требования к поставляемым продуктам:

1.1 Межсетевой экран следующего поколения

Наименование требований	Технические требования
Кол-во	2 комплекта
Тип продукта	Межсетевой экран
Форм-фактор	Установка в стандартные 19" монтажные шкафы, должен занимать не более 1U.
Количество встроенных интерфейсов	12 портов 1 Гбит/с RJ45 и 4 оптических слота 10 Гбит/с SFP+
Порты управления	Serial console port - RJ45 - не менее 1 шт
Оптические приемопередатчики	Не менее 2 кабелей со встроенными оптическими приемопередатчиками 10GBASE-CU SFP+ длиной 2м Не менее 1 кабелей со встроенными оптическими приемопередатчиками 10GBASE-CU SFP+ длиной 1м
Наличие USB 2.0 портов	Не менее 1 порта
Дисковый накопитель	Наличие SSD накопитель ёмкостью не менее 200 ГБ
Блок питания	Не менее 2 шт. мощностью не менее 400 Вт с возможностью горячей замены.
Вентиляторный модуль	Не менее 4 вентиляторов в режиме 3+1 с возможностью горячей замены
Масса устройства	Масса устройства со всеми установленными блоками питания, сетевыми модулями и блоком вентиляторов не должна превышать 9 кг.
Требования к производительности межсетевого экрана.	<ul style="list-style-type: none"> ○ Пропускная способность межсетевого экрана в режиме инспекции трафика не менее 10 Гбит/с ○ Пропускная способность межсетевого экрана в режиме инспекции трафика, контроля приложения и системы предотвращения вторжений не менее 5 Гбит/с ○ Пропускная способность межсетевого экрана в режиме IPSec VPN не менее 1 Гбит/с ○ Количество одновременных сессий не менее 2 000 000. ○ Кол-во создания новых сессий в секунду не менее 40 000 ○ Дешифрация TLS трафика не менее 730 Мбит/с
Требования к функционалу межсетевого экрана.	<ul style="list-style-type: none"> ○ Межсетевой экран следующего поколения должен поддерживать возможность использования сервисов управления работой приложений, предотвращения вторжений, фильтрации запросов пользователей по URL, предотвращения проникновения вредоносного кода (допускается активация различного функционала с помощью отдельных дополнительных подписок). ○ Поддержка развертывания как в «прозрачном» режиме, так и в режиме маршрутизации. ○ Поддержка подключения удаленных пользователей посредством SSL клиента Remote Access VPN, не менее 100 одновременных пользователей ○ Поддержка протоколов IPv4 и IPv6. ○ В частности, для протокола IPv6 поддержка в рамках правил межсетевого экрана, управления работой

Наименование требований	Технические требования
	<p>приложений, системы предотвращения вторжений, фильтрации веб-запросов пользователей по URL.</p> <ul style="list-style-type: none"> ○ Поддержка протоколов маршрутизации OSPF и BGP (версии 4 и версии 6). ○ Поддержка динамического и статического механизма трансляции сетевых адресов NAT. ○ Поддержка распознавания более 4 000 приложений с возможностью гранулярного управления функциональностью ряда приложений. ○ Возможность управления использованием приложений на уровне отдельных пользователей или групп пользователей, возможность интеграции с внешними каталогами пользователей. ○ Возможность описания приложений администратором системы с использованием стандартного для отрасли языка OpenAppID. ○ Поддержка классификации приложений по уровню риска и по уровню соответствия требованиям бизнеса. ○ Поддержка механизмов ограничения скорости передачи и обеспечения качества обслуживания. ○ Поддержка локального управления на уровне устройства и централизованного управления системой управления описанной в п. 2 настоящего документа. Доступный функционал может различаться в зависимости от выбранного варианта управления. ○ Поддержка отказоустойчивых конфигураций (активное-резервное)
<p>Требования к системе централизованного управления.</p>	<ul style="list-style-type: none"> ○ Возможность получать доступ к содержимому сетевого пакета при анализе события безопасности. ○ Встроенные механизмы создания пользовательских отчетов произвольного содержания по событиям, содержащимся в базе данных. ○ Возможность создания отчета одним щелчком с настраиваемой информационной панели. ○ Поддержка различных форматов выгрузки отчетов (PDF, HTML, CSV). ○ Возможность произвольного поиска по базе данных событий. ○ Возможность создания и сохранения пользовательских шаблонов поиска. ○ Поддержка ролевой модели управления доступом к системе централизованного управления. ○ Возможность интеграции с внешними системами аутентификации (RADIUS, LDAP, AD). ○ Поддержка открытых API для взаимодействия внешних систем с системой централизованного управления. ○ Единая платформа централизованного управления сервисами межсетевого экрана, системы предотвращения вторжений, контроля приложений, фильтрации веб-запросов пользователей по URL, платформы для предотвращения проникновения вредоносного кода.

Наименование требований	Технические требования
<p>Дополнительные требования к сервисам обеспечения информационной безопасности.</p>	<p>Требования к сервису предотвращения вторжений:</p> <ul style="list-style-type: none"> ○ Сервис предотвращения вторжений должен непрерывно оценивать состояние сети и параметры конечных устройств. Он должен использовать результаты оценки при принятии решений. ○ В процессе оценки сети сервис предотвращения вторжений должен автоматически формировать профиль конечного устройства, регистрируя операционную систему, используемые сервисы и приложения, а также определяя возможные уязвимости конечного устройства. ○ Сервис предотвращения вторжений должен автоматически определять приоритет событий безопасности в соответствии со сведениями о защищаемой среде (с учетом профиля конечного устройства и сведений о возможных уязвимостях). ○ Сервис предотвращения вторжений должен автоматически формировать рекомендации по политике предотвращения вторжений на основании результатов оценки сети. ○ Сервис предотвращения вторжений должен поддерживать задание белых списков устройств/операционных систем/приложений/сервисов. ○ Сервис предотвращения вторжений должен поддерживать возможность задания правил корреляции событий. ○ Сервис предотвращения вторжений должен поддерживать возможность инициирования действий внешними системами на основании правил корреляции. ○ Сервис предотвращения вторжений должен поддерживать обнаружение признаков компрометации конечных устройств на основании нескольких событий безопасности. ○ Сервис предотвращения вторжений должен поддерживать API для дополнения данных об конечных устройствах из других источников. ○ Сервис предотвращения вторжений должен поддерживать возможность просмотра правил/фильтров/сигнатур. ○ Сервис предотвращения вторжений должен поддерживать возможность редактирования существующих правил. ○ Сервис предотвращения вторжений должен поддерживать возможность создания пользовательских правил с использованием синтаксиса системы с открытым исходным кодом Snort. ○ Система должна поддерживать автоматическую регулярную загрузку черных и белых списков IP-адресов, URL-адресов и DNS-имен как из источников, определяемых производителем, так и из пользовательских источников.

Наименование требований	Технические требования
	<p>Требования к сервису контроля приложений.</p> <ul style="list-style-type: none"> ○ Сервис контроля приложений должен выполнять глубокую инспекцию пакетов и позволять фильтровать трафик на основе конкретных приложений. Должно быть доступно более 4000 различных приложений, включая TeamViewer, голосовые/видео приложения, почтовые приложения, file sharing, peer-to-peer торренты (P2P), игры и т.д <p>Требования к сервису фильтрации веб-запросов пользователей по URL.</p> <ul style="list-style-type: none"> ○ Сервис фильтрации должен поддерживать возможность категоризации URL и фильтрации на уровне категорий URL. ○ Сведения о различных категориях URL должны автоматически обновляться в режиме реального времени. ○ Сервис фильтрации запросов по URL должен обеспечивать фильтрацию HTTPS-запросов без расшифровки SSL-трафика. ○ Сервис фильтрации запросов должен поддерживать возможность разрешения определенным группам пользователей или пользователям «осознанно обходить» установленные правила фильтрации без вмешательства ИТ-администратора.
Подписка на обновление сигнатур сервиса предотвращения вторжений, контроля приложений и URL фильтрации	36 месяцев
Сервисная поддержка	36 месяцев

1.2 Система управления межсетевыми экранами

Наименование требований	Технические требования
Кол-во	1 комплект.
Тип продукта	Система Централизованного Управления Комплексом Межсетевых Экранов Нового Поколения
Реализация	Система должна быть реализована на базе виртуального сервера
Управление	Посредством WEB браузера через SSL
Количество МСЭ под управлением системы	Не менее 2 шт.
Требования к виртуальным ресурсам	VMware vSphere не ниже версии 6.0; не менее 4vCPU; не менее 32 ГБ оперативной памяти, не менее 250 ГБ свободного дискового пространства
Общее описание системы	<p>Система должна реализовывать функции централизованно управления, мониторинга и отчетности для комплекса решений по межсетевому экранированию нового поколения (NGFW), работающих на базе решений:</p> <ul style="list-style-type: none"> ○ Firewall Services; ○ Firewall Threat Defense; <p>Система должна предоставлять возможность настройки множественных компонент, составляющих политики</p>

Наименование требований	Технические требования
	<p>доступа, выгружаемые на группы контролируемых устройств. Компоненты должны включать, но не ограничиваться:</p> <ul style="list-style-type: none"> ○ Наборы переменных окружения для движка SNORT; ○ Объекты динамически загружаемых с сайта производителя репутационных фильтров, разбитых на категории злоумышленников, работающих как на базе информации о Доменах, так и по IP. ○ Объектов, динамически подгружаемых по расписанию с внутренних ресурсов заказчика по HTTP списков блокировки по IP/Домен/URL. ○ Политика фильтрации файлов ○ Политика фильтрации DNS запросов ○ Политика инспекции зашифрованного трафика (SSL-Decrypt) ○ Политика анализа туннелированного трафика ○ Политика обнаружения вторжений ○ Политика идентификации пользователей <p>Опции настройки для политики инспекции файлов должны включать:</p> <ul style="list-style-type: none"> ○ Возможность настройки обработки множества разных сценариев файлового анализа на основании входных параметров конкретных правил в рамках каждой отдельной политики файлового анализа. ○ Возможность выбора протокола, при передаче по которому будет проводиться инспекция файлов: <ul style="list-style-type: none"> i. HTTP ii. SMTP iii. IMAP iv. POP3 v. FTP vi. SMB ○ Возможность выбора направления передачи файла: <ul style="list-style-type: none"> i. Upload ii. Download ○ Выбор файлов, подпадающих под конкретное правило основываясь как на принадлежности типа файла к конкретному типу файлов (пример: PDF, Графические файлы, Архивы, Офисные документы и т.д.), так и на базе конкретных типов файлов (пример: pdf, msexec, binhex, xrs и т.д.) ○ Выбор действия на совпадение с критериями правила: <ul style="list-style-type: none"> i. Обнаруживать файлы и их тип ii. Блокировать файлы iii. Обнаружение вредоносного контента в файлах без блокировки iv. Обнаружение вредоносного контента в файлах с блокировкой ○ Продвинутое опции должны давать возможность установки глубины анализа архивов и возможных

Наименование требований	Технические требования
	<p>действий при обнаружении не анализируемых архивов (не раскрываемых и зашифрованных)</p> <p>Опции настройки для политик обнаружения вторжений должны включать:</p> <ul style="list-style-type: none"> ○ Возможность автоматической перенастройки сигнатурного набора с использованием рекомендаций, сгенерированных системой на основании данных, собираемых о защищаемой инфраструктуре, профилях хостов, версиях ОС, патчах, версиях приложений и составленных на основе этих данных базах уязвимостей, которым в соответствии подбирается набор защитных сигнатур. ○ Правила сигнатурного анализа должны быть написаны на языке описания сигнатур движка SNORT. <p>Опции настройки для политики идентификации пользователей должны включать:</p> <ul style="list-style-type: none"> ○ Возможность настройки обработки множества разных сценариев пользовательской идентификации на основании входных параметров конкретных правил в рамках каждой отдельной политики идентификации пользователей ○ Возможность выбора в рамках каждого конкретного правила опций соответствия зоне безопасности, сети, VLAN, Портов. <p>Система должна иметь возможность описания сигнатур определения приложений через открытый язык описания приложений OpenAppID.</p> <p>Система должна иметь встроенный мастер написания сигнатур на языке SNORT и возможность импорта собственных сигнатур из текстовых файлов</p> <p>Система должна иметь возможность использования в качестве критерия написания правил политик доступа метки безопасности SGT (Security Group Tag)</p> <p>Система должна уметь интегрироваться с системами анализа уязвимостей, которые бы поставляли данные в хостовые профили по результатам проведенного активного сканирования на уязвимости</p> <p>Система должна поддерживать интеграцию с продуктом контроля и учета доступа в сеть посредством API интерфейса.</p> <p>Система должна проводить оценку возможной успешности атаки выставляя метрику воздействия от 1 до 4-х. Метрика должна оцениваться с привязкой к целевой операционной системе, атакуемому сервису и наличия в целевой версии уязвимости, на которую направлена атака.</p>
Сервисная поддержка	36 месяцев

3.3 Коммутатор ядра сети

Наименование требований	Технические требования
Кол-во	2 комплекта
Тип продукта	Коммутатор
Форм-фактор	Установка в стандартные 19" монтажные шкафы, должен занимать не более 1U.
Сетевые интерфейсы	Не менее 48 оптических слотов 10 Gigabit Ethernet (SFP+)
Управление	Один выделенный порт управления 1Gb RJ45, один RS-232 serial console port, два USB порта
Оптические приемопередатчики	Не менее 18 модулей оптического приемопередатчика 10GBASE-LR-S-SFP+ Не менее 1 кабелей со встроенными оптическими приемопередатчиками 10GBASE-CU SFP+ длиной 1м
Блок питания	Не менее 2 блоков питания с мощностью не ниже 400 Вт с воздушным охлаждением port side exhaust и с возможностью горячей замены
Пропускная способность коммутатора	Не менее 960 Gigabit per second (Гбит/с)
Скорость пересылки пакетов	Не менее 720 million packets per second (mpps)
Общее количество MAC-адресов	Не менее 64 000
Общее кол-во unicast/multicast IPv4 маршрутов	Не менее 24 000/8000
Поддерживаемое количество записей списков доступа	Не менее 4096
Поддерживаемое количество портов агрегации	Не менее 24
Максимально поддерживаемое количество линков в одном агрегированном порту	Не менее 24
Максимально поддерживаемое количество процессов протокола разрыва петель	Не менее 512 Rapid Spanning Tree Protocol Не менее 64 Multiple Spanning Tree
Системная память	Не менее 4 ГБ
Размер буфера	Не менее 6 МБ на каждые 16 портов и не менее 18 МБ общее
Загрузочная флеш память	Не менее 4 ГБ
Поддержка Jumbo фреймов	Обязательна, размер фрейма не менее 9216 байт
Количество VLAN	Не менее 4096
Возможность объединения коммутаторов в один стек	Поддержка технологии виртуального стекирования двух коммутаторов (virtual Port Channel (vPC) или аналог)
Поддержка технологий 3-го уровня модели OSI	Inter-VLAN Routing (IVR), статическая маршрутизация, Routing Information Protocol Version 2 (RIPv2), Open Shortest Path First Version 2 (OSPFv2; до 256 маршрутов) и Virtual Router Redundancy Protocol (VRRP)
Поддержка технологий мультикаста	Multicast: Protocol-Independent Multicast Sparse Mode (PIM-SM), Source-Specific Multicast (SSM), and Multicast Source Discovery Protocol (MSDP)

Наименование требований	Технические требования
Безопасность	<ul style="list-style-type: none"> • Входящие на Ethernet списки доступа (стандартные и расширенные) • Стандартные и расширенные списки доступа 3-го и 4-го уровня модели OSI включая IPv4, Internet Control Message Protocol (ICMP), TCP и User Datagram Protocol (UDP) • Списки доступа по VLAN (VLAN-based ACLs (VACLs)) • Списки доступа на основании портов (Port-based ACLs (PACLs)) • Именные списки доступа • Списки доступа виртуальных терминалов (VTYs) • Dynamic Host Configuration Protocol (DHCP) relay • Control Plane Policing (CoPP)
Управляемость	Возможность подключения коммутатора к централизованной системе управления и мониторинга
Поддерживаемые сертификаты безопасности	IEC 60950-1 IEC 60950-1
Поддерживаемые сертификаты электромагнитной совместимости	EN61000-3-2 EN 300 386 EN55024
Сервисная поддержка	36 месяцев

3.4 Коммутатор центра обработки данных

Наименование требований	Технические требования
Кол-во	2 комплекта
Тип продукта	Коммутатор
Форм-фактор	Установка в стандартные 19" монтажные шкафы, должен занимать не более 1U.
Сетевые интерфейсы	Не менее 48 слотов 1/10/25 Gigabit Ethernet (SFP+) Не менее 6 слотов 40/100 Gigabit Ethernet (QSFP28)
Управление	Не менее 2 выделенных портов управления: 1 Gb RJ45 и 1 Gb SFP Не менее 1 порта RS-232 serial console Не менее 1 USB порта
Оптические приемопередатчики	Не менее 25 модулей оптического приемопередатчика 10GBASE-T SFP+ для связи по UTP кабелю Cat.6 на скорости 1/10 Гб/с Не менее 6 кабелей со встроенными оптическими приемопередатчиками 10GBASE-CU SFP+ длиной 1м Не менее 8 кабелей со встроенными оптическими приемопередатчиками 10GBASE-CU SFP+ длиной 2м Не менее 7 кабелей со встроенными оптическими приемопередатчиками 10GBASE-CU SFP+ длиной 3м

Наименование требований	Технические требования
Блок питания	Не менее 2 блоков питания с мощностью не ниже 650 Вт, с воздушным охлаждением port side exhaust и с возможностью горячей замены
Пропускная способность коммутатора	Не менее 3.6 Terabits per second (Tbps)
Скорость пересылки пакетов	Не менее 2.6 billion packets per second (bpps)
Общее количество MAC-адресов	Не менее 256 000
Максимальное кол-во записей IP host	Не менее 896 000
Максимальное кол-во мультикаст маршрутов	Не менее 32 000
Кол-во VRF	Не менее - Shipping: 1,000 Maximum: 16 000
Возможность подключения к коммутатору расширительных фабрик коммутации (Fabric Extenders или аналог)	Не менее 16
Поддержка многопутевой маршрутизация с равной стоимостью Equal-Cost MultiPath (ECMP)	Не менее 64 маршрутов
Поддержка агрегации портов	Не менее 32 линков в одном агрегированном порту, общее поддерживаемое кол-во агрегированных портов не менее 512
Системная память	Не менее 24 ГБ
Размер буфера	Не менее 40 МБ
Загрузочная флеш память	Не менее 64 ГБ SSD
Процессор	Не менее 4 ядер
Поддерживаемое количество записей списков доступа	Не менее 4000 (входящих), не менее 2000 (исходящих)
Поддержка Jumbo фреймов	Обязательна, размер фрейма не менее 9216 байт
Количество VLAN	Не менее 4096
Максимальное кол-во SPAN сессий	Не менее 4
Максимальное кол-во Network Address Translation (NAT) записей	Не менее 1023
Кол-во Multiple Spanning Tree (MST) instances	Не менее 64
Возможность объединения коммутаторов в один стек	Поддержка технологии виртуального стекирования двух коммутаторов (virtual Port Channel (vPC) или аналог)
Поддерживаемые функциональные технологии	Статическая маршрутизация, switch virtual interfaces (SVIs), Virtual Router Redundancy Protocol (VRRP) и Routing Information Protocol (RIP)
Управляемость	Возможность подключения коммутатора к централизованной системе управления и мониторинга
Поддерживаемые сертификаты безопасности	IEC 60950-1 IEC 60950-1
Поддерживаемые сертификаты электромагнитной совместимости	EN61000-3-2 EN 300 386 EN55024
Сервисная поддержка	36 месяцев

3.5 Коммутаторы доступа тип 1.

Наименование требований	Технические требования
Кол-во	4 комплекта
Тип продукта	Коммутатор
Форм-фактор	Для монтажа в шкаф, высотой не более 1U.
Порты	Не менее 48 портов Gigabit Ethernet (RJ45) Не менее 4 слота 10 Gigabit Ethernet (SFP+)
Пропускная способность	Не менее 170 Гб/с
Производительность	Не менее 130 млн пакетов в сек
Общее количество MAC-адресов (Unicast)	Не менее 16 000
Количество маршрутов IPv4 (static)	Не менее 542
Количество маршрутов IPv6 (static)	Не менее 414
DRAM	Не менее 512 МБ
Flash	Не менее 256 МБ
Количество VLAN	Не менее 4094
Поддерживаемые средства информационной безопасности	<ul style="list-style-type: none"> • IEEE 802.1X • Поддержка списков доступа (ACLs) • Поддержка списков на основании порта (Port-based ACLs) • SSH, Kerberos, SNMP v3 (для защиты сеансов работы администратора) • SPAN • Аутентификация TACACS+ RADIUS • Фильтрация Internet Group Management Protocol (IGMP) • Динамическое назначение VLAN
Обеспечение доступности и отказоустойчивости	<ul style="list-style-type: none"> • Rapid Spanning Tree Protocol (RSTP) • Multiple Spanning Tree Protocol (MSTP)
Обеспечение QoS	<ul style="list-style-type: none"> • 802.1p Class of Service • Voice VLAN (для выделения голосового трафика в отдельный VLAN)
Управляемость	Устройства должны поддерживать совместимость с централизованной системой управления и мониторинга.
Сертификаты безопасности	IEC 62368-1
Сертификат электромагнитной совместимости	EN 61000-3-2, EN 300386
Сервисная поддержка	36 месяцев

3.6 Коммутаторы доступа тип 2.

Наименование требований	Технические требования
Кол-во	2 комплекта
Тип продукта	Коммутатор
Форм-фактор	Для монтажа в шкаф, высотой не более 1U.
Порты	Не менее 8 портов Gigabit Ethernet (RJ45) Не менее 2 порта Gigabit Ethernet (RJ45) в комбо режиме с 2 слотами Gigabit Ethernet (SFP)
Пропускная способность	Не менее 20 Гб/с

Наименование требований	Технические требования
Производительность	Не менее 14 млн пакетов в сек
Общее количество MAC-адресов (Unicast)	Не менее 16 000
Количество маршрутов IPv4 (static)	Не менее 542
Количество маршрутов IPv6 (static)	Не менее 414
DRAM	Не менее 512 МБ
Flash	Не менее 256 МБ
Количество VLAN	Не менее 4094
Поддерживаемые средства информационной безопасности	<ul style="list-style-type: none"> • IEEE 802.1X • Поддержка списков доступа (ACLs) • Поддержка списков на основании порта (Port-based ACLs) • SSH, Kerberos, SNMP v3 (для защиты сеансов работы администратора) • SPAN • Аутентификация TACACS+ RADIUS • Фильтрация Internet Group Management Protocol (IGMP) • Динамическое назначение VLAN
Обеспечение доступности и отказоустойчивости	<ul style="list-style-type: none"> • Rapid Spanning Tree Protocol (RSTP) • Multiple Spanning Tree Protocol (MSTP)
Обеспечение QoS	<ul style="list-style-type: none"> • 802.1p Class of Service • Voice VLAN (для выделения голосового трафика в отдельный VLAN)
Управляемость	Устройства должны поддерживать совместимость с централизованной системой управления и мониторинга.
Сертификаты безопасности	IEC 62368-1
Сертификат электромагнитной совместимости	EN 61000-3-2, EN 300386
Сервисная поддержка	36 месяцев

3.7 Коммутатор системы управления

Наименование требований	Технические требования
Кол-во	1 комплект
Тип продукта	Коммутатор
Форм-фактор	Для монтажа в шкаф, высотой не более 1U.
Порты	Не менее 48 портов Gigabit Ethernet (RJ45) Не менее 4 слота Gigabit Ethernet (SFP)
Пропускная способность	Не менее 104 Гб/с
Производительность	Не менее 77 млн пакетов в сек
Общее количество MAC-адресов (Unicast)	Не менее 16 000
Количество маршрутов IPv4 (static)	Не менее 542
Количество маршрутов IPv6 (static)	Не менее 414
DRAM	Не менее 512 МБ
Flash	Не менее 256 МБ
Количество VLAN	Не менее 4094

Наименование требований	Технические требования
Поддерживаемые средства информационной безопасности	<ul style="list-style-type: none"> • IEEE 802.1X • Поддержка списков доступа (ACLS) • Поддержка списков на основании порта (Port-based ACLs) • SSH, Kerberos, SNMP v3 (для защиты сеансов работы администратора) • SPAN • Аутентификация TACACS+ RADIUS • Фильтрация Internet Group Management Protocol (IGMP) • Динамическое назначение VLAN
Обеспечение доступности и отказоустойчивости	<ul style="list-style-type: none"> • Rapid Spanning Tree Protocol (RSTP) • Multiple Spanning Tree Protocol (MSTP)
Обеспечение QoS	<ul style="list-style-type: none"> • 802.1p Class of Service • Voice VLAN (для выделения голосового трафика в отдельный VLAN)
Управляемость	Устройства должны поддерживать совместимость с централизованной системой управления и мониторинга.
Сертификаты безопасности	IEC 62368-1
Сертификат электромагнитной совместимости	EN 61000-3-2, EN 300386
Сервисная поддержка	36 месяцев

2. Прочие условия

4.1 Предлагаемые продукты (далее товар) должны быть от известных мировых производителей (Brand Name). Все поставляемые товары должны быть новыми и не бывшими в употреблении, а также не снятыми с производства, не иметь дефектов.

4.2 В настоящее время в сети передачи данных РТСБ используется телекоммуникационное оборудование производства компаний *Cisco Systems, Extreme*. При составлении предложения необходимо учесть совместимость с эксплуатируемой системой, наличие обученного персонала. При необходимости нужно будет организовать обучение специалистов Покупателя по поставляемым продуктам.

4.3 Технические параметры продуктов должны быть не ниже затребованных. Поставщик гарантирует и обеспечивает полную комплектацию всех предлагаемых продуктов.

4.4 Поставщик должен иметь оригиналы или заверенные копии авторизационных документов от производителей продукции, подтверждающие полномочие участника на продажу предлагаемых продуктов в рамках данного проекта.

4.5 Сервисная поддержка на поставляемые продукты – 36 месяцев.

Условия сервисной поддержки поставляемых программно-аппаратных комплексов:

Сервисная поддержка производителем поставляемого программного и аппаратного обеспечения в течение 36 месяцев, обеспеченная соответствующим сервисным контрактом;

- Наличие в Ташкенте контролируемого производителем сервисного склада запасных частей и устройств для обеспечения замены устройств и частей, вышедших из строя;
- Замена неисправного оборудования в течение 36 месяцев от даты поставки программно-аппаратного обеспечения с доставкой не позже, чем следующий рабочий день с момента принятия решения о необходимости замены;
- Получение основных и промежуточных релизов программного обеспечения с официального сайта производителя;
- Постоянный (в круглосуточном режиме) авторизованный доступ к сайту производителя;

- Постоянный (в круглосуточном режиме) доступ к службе технической поддержки производителя через веб-сайт, по электронной почте и по телефону для решения проблем и эскалаций критических проблем (после сообщения о любой аппаратной, конфигурационной или программной проблеме).

4.6 Поставщик обязан выполнить монтажные и пуско-наладочные работы по запуску программно-аппаратных комплексов в опытную эксплуатацию на основании согласованных методик приемо-сдаточных испытаний

Условия по монтажу и пуско-наладке:

- Заказчик разрабатывает и согласовывает с поставщиком методику приемо-сдаточных испытаний по вводу программно-аппаратных комплексов в эксплуатацию
- Работы по вводу программно-аппаратных комплексов должны выполняться специалистами, сертифицированными производителем.
- Заказчик обязан предоставить специалистам поставщика всю необходимую информацию и доступ к помещениям и продуктам для выполнения работ.

4.7 В техническом предложении (форма №2) Участник тендера должен указать:

- артикул (Part number), наименование и основные характеристики поставляемого продукта;
- год производства поставляемого оборудования;
- страну происхождения поставляемого оборудования;
- завод изготовителя;
- срок поставки;
- условия поставки.

приложение №1

Общая информация об участнике тендера

1.	Полное наименование юридического лица, с указанием организационно-правовой формы	
2.	Прежнее, полное наименование юридического лица, с указанием организационно правовой формы	
3.	Сведения о регистрации (дата регистрации, регистрационный номер, наименование регистрирующего органа)	
4.	Юридический адрес	
5.	Контактный телефон, факс, e-mail	
6.	ИНН	
7.	ОКЭД	
8.	Банковские реквизиты для оплаты по результатам данного тендера	
9.	Основные направления деятельности	

<hr/> <i>(подпись уполномоченного лица)</i>	<hr/> <i>(Ф.И.О. и должность уполномоченного лица)</i>
---	--

М.П.

Дата: «__» _____ 2021г.

приложения №2

Техническое предложение по тендеру: “Модернизация существующей сети передачи данных РТСБ Республики Узбекистан”

Межсетевой экран следующего поколения 2 комплекта				
Артикул (Part Number)	Наименование	Завод изготовитель	Год производства	Срок гарантии
Система управления межсетевыми экранами 1 комплект				
Артикул (Part Number)	Наименование	Завод изготовитель	Год производства	Срок гарантии
Коммутатор ядра сети 2 комплекта				
Артикул (Part Number)	Наименование	Завод изготовитель	Год производства	Срок гарантии
Коммутатор центра обработки данных 2 комплекта				
Артикул (Part Number)	Наименование	Завод изготовитель	Год производства	Срок гарантии
Коммутатор доступа Тип 1 4 комплекта				
Артикул (Part Number)	Наименование	Завод изготовитель	Год производства	Срок гарантии

Коммутатор доступа Тип 2 2 комплекта				
Артикул (Part Number)	Наименование	Завод изготовитель	Год производства	Срок гарантии
Коммутатор системы управления 1 комплект				
Артикул (Part Number)	Наименование	Завод изготовитель	Год производства	Срок гарантии

Срок поставки – в течении ____ дней. Условия поставки.

Монтажные и пуско-наладочные работы по запуску поставленных программно-аппаратных комплексов в опытную эксплуатацию

Срок выполнения работ – в течении ____ дней.

(подпись уполномоченного лица)

(Ф.И.О. и должность уполномоченного лица)

М.П.

Дата: «__» _____ 2021г.

приложения №3

Таблица соответствия по тендеру: “Модернизация существующей сети передачи данных РТСБ Республики Узбекистан”

Межсетевой экран следующего поколения 2 комплекта				
Требуемое в соответствии с п.3.1 Технических условий		Предложение участника тендера		
Характеристика	Значение	Характеристика	Значение	Соответствует/ Не соответствует
Система управления межсетевыми экранами 1 комплект				
Требуемое в соответствии с п.3.2 Технических условий		Предложение участника тендера		
Характеристика	Значение	Характеристика	Значение	Соответствует/ Не соответствует
Коммутатор ядра сети 2 комплекта				
Требуемое в соответствии с п.3.3 Технических условий		Предложение участника тендера		
Характеристика	Значение	Характеристика	Значение	Соответствует/ Не соответствует
Коммутатор центра обработки данных 2 комплекта				
Требуемое в соответствии с п.3.4 Технических условий		Предложение участника тендера		
Характеристика	Значение	Характеристика	Значение	Соответствует/ Не соответствует

Коммутатор доступа Тип 1 4 комплекта				
Требуемое в соответствии с п.3.5 Технических условий		Предложение участника тендера		
Характеристика	Значение	Характеристика	Значение	Соответствует/ Не соответствует
Коммутатор доступа Тип 2 2 комплекта				
Требуемое в соответствии с п.3.6 Технических условий		Предложение участника тендера		
Характеристика	Значение	Характеристика	Значение	Соответствует/ Не соответствует
Коммутатор системы управления 1 комплект				
Требуемое в соответствии с п.3.7 Технических условий		Предложение участника тендера		
Характеристика	Значение	Характеристика	Значение	Соответствует/ Не соответствует

(подпись уполномоченного лица)

(Ф.И.О. и должность уполномоченного лица)

М.П.

Дата: «__» _____ 2021г.