Общество с ограниченной ответственностью

«Исполнитель»

**ТЕХНО-РАБОЧИЙ ПРОЕКТ**

**Система обеспечения информационной безопасности**

**Подсистема межсетевого экранирования**

**ООО «Рога и копыта»**

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**Москва**

**2024**

АННОТАЦИЯ

Настоящий документ содержит описание технических решений по созданию подсистемы межсетевого экранирования **ООО «Рога и копыта»** (далее — ПМЭ / Подсистема).

Документ описывает комплекс организационных и технических мероприятий, реализуемых в рамках создаваемой Подсистемы, основные характеристики Подсистемы и порядок ее функционирования.

Документ разработан в соответствии с ГОСТ Р 2.105-2019 «Единая Подсистема конструкторской документации. Общие требования к текстовым документам» и ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные Подсистемы. Автоматизированные Подсистемы. Требования к содержанию документов».

# Общие положения

## Наименование проектируемой Подсистемы и наименования документов, на основании которых ведётся проектирование

Полное наименование проектируемой Подсистемы: Подсистема межсетевого экранирования ООО «Рога и копыта».

Сокращенное наименование Подсистемы: Подсистема / ПМЭ.

Основанием для выполнения работ является: Договор № 322 от «30» сентября 2023 года между ООО «Рога и копыта» и ООО «Исполнитель».

## Перечень организаций, участвующих в разработке Подсистемы, сроки выполнения стадий

**Заказчиком** является ООО «Рога и копыта» (далее - ООО «РиК»).

**Юридический адрес:** 000000, ул. Красивой документации, дом 8

**Исполнителем** работ является ООО «Исполнитель».

**Юридический адрес:** 000000, ул. Красивой документации, дом 8

## Назначение и область использования Подсистемы

Подсистема межсетевого экранирования предназначена для:

* анализа, контроля и фильтрации сетевых пакетов;
* разграничения сетей с различным уровнем доверия;
* идентификации, анализа ии контроля передачи данных сетевых приложений;
* идентификации и аутентификации пользователей;
* обнаружения и предотвращения вторжений и вредоносной активности в сети;
* ограничения доступа к подозрительным сайтам;
* построения защищенных каналов связи;
* управления политиками безопасности;
* централизованого управления и мониторинга.

Подсистема обеспечивает сетевую безопасность корпоративной ИТ-инфраструктуры Заказчика. Подсистема преднзначена для обеспечения многоуровневой защиты сетевого периметра и внутренних сегментов сети Заказчика от продвинутых сетевых угроз путем комплексного использования различная функция сетевой безопасности

Областью использования Подсистемы является информационно-телекоммуникационная инфраструктура (далее - ИТИ) Заказчика, расположенная на территории Заказчика по адресу: 000000, ул. Красивой документации, дом 8

## Предпосылки, цель и задачи внедрения

Основной целью внедрения ПМЭ ООО «РиК» является повышение стабильности деятельности Заказчика за счет снижения времени прерывания бизнес-процессов вследствие наступления инцидентов информационной безопасности.

Настоящая цель должна достигаться за счет:

* предупреждения и сокращения времени обнаружения инцидентов информационной безопасности и ликвидации их последствий, а также повышения степени готовности ИТИ в целом для обеспечения безопасности информационных и бизнес-процессов;
* повышения эффективности работы функции информационной безопасности.

ПМЭ должна обеспечивать решение следующих общих задач:

* фильтрации данных, передаваемых по сетевым каналам связи и контроля доступа к различным сегментами сети, в т.ч. на уровне пользователей и приложений;
* обнаружения и предотвращения сетевых угроз на уровне периметра ИТИ
* обеспечения безопасности информации при ее передаче за пределы периметра ИТИ
* регистрации событий информационной безопасности и ее передачи во внешние системы
* предоставление интерфейса для централизованного управления политиками сетевой безопасности.

## Общая характеристика объектов контроля

Объектами контроля ПМЭ являются исходящие и входящие данные передаваемые по каналам связи локальной вычислительной сетях (далее – сетевой трафик) ресурсов ИТИ обеспечивающих функционирование бизнес-систем, офисных систем, телекоммуникационных систем в интересах клиентов и функциональных подразделений Заказчика, а также систем оперативного управлению инфраструктурой и систем специального назначения (далее – устройства сети).

## Сведения об использованных при проектировании нормативно-технических документах

Проектирование Подсистемы осуществляется с учетом требований комплекса государственных стандартов «Информационная технология. Комплекс стандартов на автоматизированные Подсистемы»:

1. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные Подсистемы. Автоматизированные Подсистемы. Стадии создания»
2. ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные Подсистемы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
3. ГОСТ 34.602 2020 «Информационные технологии. Комплекс стандартов на автоматизированные Подсистемы. Техническое задание на создание автоматизированной Подсистемы»
4. Гост Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные Подсистемы. Автоматизированные Подсистемы. Термины и определения»
5. ГОСТ Р 59792-2021 «Информационные технологии. Комплекс стандартов на автоматизированные Подсистемы. Виды испытаний автоматизированных систем»;
6. ГОСТ Р 59795-2019 «Информационные технологии. Комплекс стандартов на автоматизированные Подсистемы. Автоматизированные Подсистемы. Требования к содержанию документов».

# Описание процесса деятельности Подсистемы

## Описание процесса деятельности

Подсистема предназначена для обеспечения многоуровневой защиты сетевого периметра и внутренних сегментов сети Заказчика от продвинутых сетевых угроз путем комплексного использования различных функций сетевой безопасности.

Процесс деятельности Подсистемы включает следующие автоматизированные и не автоматизированные процедуры:

1. Устройства сети, расположенные в рамках ИТИ, и удаленные устройства формируют сетевой трафик в процессе сетевого взаимодействия, происходящего в ИТИ.
2. Сетевой трафик проходит через ПМЭ, где происходит его анализ и фильтрация.
3. В ходе анализа выявляются угрозы ИБ в составе сетевого трафика. В случае, если угрозы будут отнесены ПМЭ к разряду инцидентов, происходит формирование соответствующего сообщения и проводится информирование персонала (администраторов) ПМЭ, при этом также могут запускаться настроенные сценарии реагирования.
4. Получив сообщение об инциденте, персонал анализирует полученное сообщение и, в случае необходимости, принимает меры, направленные на устранение возникшего инцидента.
5. После устранения возникшего инцидента и ликвидации его последствий осуществляется выявление причин возникновения инцидента.
6. На основе знания о причинах возникновения инцидента разрабатывается комплекс мер, направленных на недопущение повторения ситуации, приведшей к возникновению инцидента.

## Описание среды функционирования Подсистемы

Для проведения работ по проектированию Подсистемы было проведено обследование (интервьюирование специалистов Заказчика) с целью изучения состава ИТИ, процессов управления и обеспечения ИБ Заказчика, изучения процессов обработки информации.

В результате обследования ИТИ Заказчика разработан настоящий документ и отчетные документе этапа 1, а именно:

* схема сетевого взаимодействия и информационных потоков;
* монтажная схема;
* сетевая схема (HLD, LLD);
* кабельный журнал.

## Исходные данные

Режим работы ПМЭ – High Availability, Active/Passive mode (далее – кластер).

Пропускная способность кластера в режиме Firewall – до 7,5 Гбит/сек.

Пропускной способности кластера в режиме IPS – до 5,5 Гбит/сек.

Пропускная способность кластера в режиме NGFW – до 5 Гбит/сек.

Пропускная способность кластера в режиме NGTP – до 2 Гбит/сек.

При увеличение нагрузки обеспечиваются меры по масштабированию и распределению нагрузки Подсистема (см. раздел 3.8 настоящего документа).

# ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

## Описание структуры Подсистемы

ПМЭ располагается на базе ЦОД ООО «РиК».

ПМЭ представляет собой автономную инсталяцию с единым центром управления, включающим в себя интерфейс администраторов ПМЭ.

В рамках ПМЭ проектными решениями реализован контур автоматизированного управления. Реализация контура автоматизированного управления обеспечивается средствами АПК ПМЭ.

Предусмотрено резервирование узлов ПМЭ в режиме высокой доступности (High-Availability).

Подсистема строится на базе программно-аппаратного комплекса Check Point Next Generation Firewall разработки компании «Check Point Software Technologies Ltd.» (далее – CheckPoint NGFW).

В состав ПМЭ входят следующие основные компоненты:

* система централизованного управления CheckPoint Smart-1 600-S;
* межсетевой экран нового поколения CheckPoint Quantum Spark 1800 Security Gateways;

Кроме того, в ПМЭ выделяется АРМ администратора информационной безопасности (далее – АПМ АИБ).

Таблица 1 – Функциональные компоненты ПМЭ

|  |  |  |
| --- | --- | --- |
| № | Наименование компонента | Функции компонента |
| Основные компоненты | | |
| 1 | CheckPoint Smart-1 600-S | Система централизованного управления CheckPoint Smart-1 модель 600-S выполняет следующие функции:   * централизованная настройка и конфигурация объектов ПМЭ; * централизованное управление политиками безопасности; * предоставление графического интерфейса для управления политиками безопасности администраторам; * определение глобальных правил безопасности и их распространение на домены управления; * централизованное управление политиками VPN в нескольких доменах управления; * … |
| 3 | Межсетевой экран нового поколения CheckPoint Quantum Spark 1800 Security Gateways | Межсетевой экран нового поколения CheckPoint Quantum Spark 1800 Security Gateways выполняет следующие функции:   * межсетевое экранирование; * построение защищенных каналов связи (VPN); * защищенный мобильный доступ (L3VPN, SSL/TLS VPM) * идентификация и аутентификация пользователей; * идентификация содержимого файлов, типов данных и их контроль; * контроль приложений; * …. |
| АРМ АИБ | | |
| 5 | АРМ АИБ | АРМ АИБ обеспечивает доступ к компонентам ПМЭ для администрирования |

В ПМЭ входят следующие компоненты CheckPoint NGFW:

* система централизованного управления CheckPoint Smart-1 600-S – 1 шт.;
* межсетевой экран нового поколения CheckPoint Quantum Spark 1800 Security Gateways – 2 шт.

### Описание основных компонентов Подсистемы

#### **Компонент CheckPoint Smart-1 600-S**

CheckPoint Smart-1 600-S – является компонентом управления ПМЭ который поставляется в виде программно-аппаратного комплекса (далее - ПАК) и решает задачу централизованного управления безопасностью сети, объединяя все компоненты ПМЭ в единое универсальное масштабируемое техническое решение для управления политиками, отслеживания угроз и общего повышения уровня устойчивости ИБ по всей инфраструктуре в целом.

Технические характеристики центра управления приведены в таблице Таблица 2.

Таблица 2

| **Параметр** | **Значение** |
| --- | --- |
| Количество управляемых шлюзов |  |
| Количество принимаемых событий в секунду |  |
| Объем, требуемый для хранения событий |  |
| ОЗУ |  |
| HDD |  |
| Встроенные интерфейсы |  |
| Блок питание |  |
| Энергопотребление (усредненное) |  |
| Габаритные размеры (ВxШxГ), мм |  |
| Форм-фактор |  |

#### **Компонент CheckPoint Quantum Spark 1800 Security Gateways**

CheckPoint Quantum Spark 1800 Security Gateways – является шлюзом безопасности, представленным в виде ПАК и предназначенным для обеспечения функций сетевой безопасности: сегментирования, защиты от современных угроз, предотвращения известных и неизвестных сетевых атак нулевого дня и других сетевых угроз, инспектирования SSL/TLS трафика, организации удаленного доступа посредством VPN типа «site-to-site» и/или «client-to-site», веб-безопасности и отказоустойчивости.

Технические характеристики CheckPoint Quantum Spark 1800 Security Gateways приведены в таблице Таблица 3.

Таблица 3 – Характеристики CheckPoint Quantum Spark 1800 Security Gateways

| **Параметр** | **Значение** |
| --- | --- |
| Количество порты |  |
| Пропускная способность в режиме МСЭ |  |
| Пропускная способность в режиме NGFW |  |
| Пропускная способность в режиме NGTP |  |
| Пропускная способность в режиме IPS |  |
| Пропускная способность в режиме VPN AES-128 |  |
| Количество устанавливаемых соединений в секунду |  |
| Общее количество установленных соединений |  |
| ОЗУ |  |
| HDD |  |
| Количество виртуальных систем |  |
| Блок питания |  |
| Энергопотребление (усредненное) |  |
| Габаритные размеры (ВxШxГ), мм |  |
| Форм-фактор |  |

#### **АПМ Администратора безопасности**

АРМ Администратора безопасности обеспечивает доступ с помощью веб-интерфейса, SmartConsole, CLI или API для предоставления администратору информационной безопасности доступа к данным и функциям ПМЭ.

### Решения по взаимодействию между компонентами Подсистемы

#### **Схема взаимодействия компонентов Подсистемы**

Порядок взаимодействия основных компонентов ПМЭ и их информационных потоков представлен на рисунке Рисунок 1.



Рисунок 1.

#### **Параметры сетевого взаимодействия компонентов Подсистемы**

Компоненты ПМЭ связаны между собой и с внешними системами локальной сетью. В качестве основного транспортного протокола для связи используется стек протоколов TCP/IP.

Для взаимодействия компонентов ПМЭ обеспечивается передача данных по портам и протоколам, указанным в Приложении ПРИЛОЖЕНИЕ В ТАБЛИЦА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ КОМПОНЕНТОВ ПОДСИСТЕМ, а также представленным на схеме сетевого взаимодействия и информационных потоков в документе «Схема сетевого взаимодействия и информационных потоков».

## Решения по взаимосвязям Подсистемы со смежными системами

ПМЭ интегрируется с нижеуказанными системами Заказчика:

1. Служба каталогов (LDAP);
2. Система мониторинга статусов оборудования;
3. Электронная почта (для уведомлений);
4. Служба каталога и служба DMS и NTP.

Взаимодействие со смежными подсистемами указано в Приложение Б.

## Режимы функционирования Подсистемы

Режим функционирования ПМЭ – автоматизированный, под управлением Администратора безопасности.

ПМЭ осущетствляет работу в следующих режимах:

* штатный режим;
* технологический режим;
* аварийный режим.

## Численность, функции и квалификация персонала

Предусматриваются следующие роли персонала, осуществляющего эксплуатацию и обслуживание ПМЭ: Администратор.

Таблица 4

|  |  |  |
| --- | --- | --- |
| Площадка | Кол-во, человек | Роли |
| ЦОД ООО «РиК» | 2 | Администратор |

## Обеспечение заданных в техническом задании потребительских характеристик Подсистемы, определяющих ее качество

Принятые решения по структуре ПМЭ, порядку взаимодействия между компонентами, взаимосвязям со смежными системами, решения по комплексу технических и программных средств обеспечивают выполнение Подсистемы своих функций.

### Обеспечение требований к показателям назначения

ПМЭ обеспечивает следующие показатели назначения:

* пропускная способность кластера в режиме Firewall – до 7,5 Гбит/сек
* пропускная способность кластера в режиме IPS – до 5,5 Гбит/сек
* пропускная способность кластера в режиме NGFW – до 5 Гбит/сек
* пропускная способность кластера в режиме NGTP – до 2 Гбит/сек.

### Надежность и отказоустойчивость Подсистемы

Отказоустойчивость ПМЭ обеспечивается на программном и аппаратном уровнях.

В составе ПМЭ используются отказоустойчивый кластер из двух аппаратных комплексов сводя к минимуму риски и время простоя за счет резервирования друг друга в режим Active/Passive.

### Лингвистическое обеспечение Подсистемы

Эксплуатационная документация, графический интерфейс пользователя и формируемые Системой отчеты выполнены на английском языке.

## Состав функций, реализуемых ПЭМ

ПМЭ с использованием функциональных компонентов, указанных в п. 3.1.1 настоящего документа обеспечивает реализацию следующих функций:

* защиту сети, контроль и фильтрацию входящего и исходящего трафика;
* систему предотвращения вторжений (IPS);
* антивирусную защиту и анти-бот;
* веб-фильтрацию и контроль приложений;
* управление VPN-сетями;
* защита от спама и электронной почты;
* аутентификацию и авторизацию пользователей;
* мониторинг и анализ трафика;
* управление политиками безопасности.

## Решения по комплексу технических средств ПМЭ

ПМЭ интегрируется в имеющуюся сетевую Border/Core/L2-access архитектуру ИТИ Заказчика в виде автономной инсталляции с центром управления путем отказоустойчивого подключения с помощью агрегации интерфейсов (LACP) компонентов ПМЭ к Cisco (VSWCOR01), функционирующему в роли ядра сети ИТИ Заказчика:

Подробная информация о монтаже, коммутации и адресации сети приведена в разделах 3.7.1.

Получение входящего и исходящего сетевого трафика с устройств сети осуществляется путем перенаправления (маршрутизации) сетевого трафика с помощью ядра сети на оборудование ПМЭ для последующего анализа и фильтрации.

После анализа и фильтрации ПМЭ осуществляет перенаправление обработанного трафика обратно на ядро сети для его последующего прохождения в адрес назначения.

Маршрутизация, с использованием статических маршрутов, настраивается таким образом, чтобы трафик ходил в обе стороны через ПМЭ. Настройки статической маршрутизации предоставлены в Приложении ПРИЛОЖЕНИЕ Д. НАСТРОКИ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ OSPF

Для обеспечения связи между внешней и внутренней сетями осуществляет множественное преобразование IP-адресов и портов с использованием функция Network Address Translation (далее – NAT). Это позволяет множеству устройств внутри локальной сети использовать один общий IP-адрес для взаимодействия с внешними сетями. Настройки NAT предоставлены в Приложении .

Таблица сетевого взаимодействия компонентов ПМЭ указана в Приложении А.

Настройки политик компонентов ПМЭ указаны в Приложении ПРИЛОЖЕНИЕ Е. НАСТРОЙКИ ПМЭ

### Описание комплекса технических средств ПМЭ

Комплекс технических средств ПМЭ, должен быть смонтирован в серверные стойки в соответствии с таблицей Таблица 5, а также схемой размещения, указанной в документе «Монтажный схема».

Таблица 5 – Размещение КТС в ЦОД ООО «РиК»

| **Место** | **Адрес** | **Номер стойки** | **Модель оборудования** | **Условное обозначение** | **Юнит** |
| --- | --- | --- | --- | --- | --- |
| ЦОД, ООО «РиК» |  | 2 | CheckPoint Quantum Spark 1800 | ITG-CP-GW-01 | X |
| 2 | ITG-CP-GW-02 | X |
| 2 | CheckPoint Smart-1 600-S | ITG-CP-SMS-01 | X |

## Решения по масштабированию Подсистемы

Комплекс ПМЭ строится с учетом дальнейшего масштабирования. Используемые компоненты имеют достаточный запас свободных портов для подключения новых узлов, а также запас по производительности, позволяющий увеличить пропускную способность.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

| Обозначение | Описание |
| --- | --- |
| АПК | Аппаратно-программный комплекс |
| АРМ | Автоматизированное рабочее место |
| КТС | Комплекс технических средств |
| Заказчик | ООО «РиК» |
| ИБ | Информационная безопасность |
| ИС | Информационная система |
| Исполнитель | ООО «Исполнитель» |
| ИТИ | Информационно-телекоммуникационная инфраструктура |
| ЦОД |  |
| ООО | Общество с ограниченной ответственностью |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| ПМЭ, Подсистема |  |
| ЦП | Центральный процессор |
| API | Application Programming Interface, интерфейс программирования приложений |
| DMS | Domain Name System, Подсистема доменных имен |
| HLD | High-level design, верхнеуровневое описание архитектуры системы |
| IPS | Intrusion Prevention System, система предотвращения вторжений |
| LDAP | Lightweight Directory Access Protocol, Протокол доступа к службе каталогов |
| LLD | Low-level design, низкоуровневое детальное описание системы |
| MGMT | Management, интерфейс управления |
| NGDP | Next Generation Data Protection |
| NGFW |  |
| NGTP | Next Generation Threat Prevention |
| NTP | Network Time Protocol, протокол сетевого времени |
| SIC | Security Internal Communication, внутреннее безопасное соединение |
| SMS | Security Management Server, сервер управления безопасностью |
| SMTP | Simple Mail Transfer Protocol, простой протокол передачи почты |
| SSL | Secure sockets layer, слой защищенных сокетов |
| TCP | Transmission Control Protocol, протокол управления передачей данных |
| TLS | Transport layer security, протокол защиты транспортного уровня |
| VPN | Virtual private network, виртуальная частная сеть |
| UDP | User Datagram Protocol, протокол пользовательских датаграмм |
| URL | Uniform Resource Locator, унифицированный указатель ресурса |

ПЕРЕЧЕНЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

|  |  |  |
| --- | --- | --- |
| Агрегация | − | процесс объединения повторяющихся событий, описывающих один и тот же инцидент. |
| Актив | − | потенциальный или действительный источник (участник) событий. Активом может быть любое управляемое реальное или виртуальное устройство информационной Подсистемы (сервер, рабочая станция, сетевое устройство), либо информационный сервис. |
| Инцидент | − | единичное либо комплексное нелегитимное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких событий), которое может скомпрометировать бизнес-процессы компании или угрожает ее информационной безопасности. |
| Компонент | − | часть Подсистемы, рассматриваемая как единое целое с точки зрения развертывания и обновления. Компоненты функционально связаны между собой, однако независимы в плане запуска. |
| Корреляция | − | процесс сопоставления значений полей событий ИБ с базой данных значений полей событий, или последовательности событий, являющихся признаками инцидента. |
| Событие информационной безопасности | − | идентифицированное появление определенного состояния Подсистемы, сервиса или сети, указывающего (напрямую или косвенно) на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к информационной безопасности. |
| Узел | − | устройство, соединённое с другими устройствами как часть компьютерной сети. Узлом может быть рабочая станция, сервер или сетевое оборудование, такое как маршрутизатор, коммутатор. |

# ПРИЛОЖЕНИЕ А. ТАБЛИЦА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ КОМПОНЕНТОВ ПМЭ

Таблица А.1- Таблица сетевого взаимодействия компонентов ПМЭ

| **Источник  FQDN/IP** | **Назначение  FQDN/IP** | **Порт** | **Примечание** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

ПРИЛОЖЕНИЕ Б. ТАБЛИЦА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ СО СМЕЖНЫМИ ПОДСИСТЕМАМИ

Таблица Б.1- Таблица сетевого взаимодействия компонентов ПМЭ

| **Сетевое взаимодействие компонентов CheckPoint** | | | | |
| --- | --- | --- | --- | --- |
| **Источник  FQDN/IP** | **Назначение  FQDN/IP** | **Порт** | **Примечание** |
| **ЦОД ООО «РиК»** | | | | |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |
|  |

# ПРИЛОЖЕНИЕ В ТАБЛИЦА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ КОМПОНЕНТОВ ПОДСИСТЕМЫ

Таблица В.1 - Взаимодействия компонентов Подсистем

| **Протокол** | **Порт** | **Имя службы/комментарий** | | **Описание** | |
| --- | --- | --- | --- | --- | --- |
| **Security Management** | | | | | |
|  |  |  | |  | |
|  |  |  |  | | |
|  |  |  | | |  |
| **Firewall** | | | | | |
|  |  |  | |  | |
|  |  |  | |  | |
|  |  |  | |  | |
| **Infrastructure** | | | | | |

ПРИЛОЖЕНИЕ Г. ДОСТУПНЫЕ ПОКАЗАТЕЛИ МЕТРИК

Таблица Г.1. Доступные основные показатели метрик

| **Обозначение метрики** | **Описание метрики** | |
| --- | --- | --- |
| **Система** | | |
| ***CPU*** | | |
|  | |  |
|  |  | |
|  |  | |

# ПРИЛОЖЕНИЕ Д. НАСТРОКИ СТАТИЧЕСКОЙ МАРШРУТИЗАЦИИ

Таблица Д. 4. Настройки статической маршрутизации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Сетевой адрес** | **Маска сети** | **Метрика** | **Интерфейс** |
|  | 0.0.0.0 | 0.0.0.0 | 1 |  |
|  | 0.0.0.0 | 0.0.0.0 | 2 |  |
|  | 10.0.0.0 | 255.0.0.0 | 1 |  |

# ПРИЛОЖЕНИЕ Е. НАСТРОЙКИ ПМЭ

Таблица Ж. 1. Глобальная политика ПМЭ

**ЛИСТ СОГЛАСОВАНИЯ**

| **№ п/п** | **ФИО** | **Должность** | **Дата** | **Подпись** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 16. |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |